TOO MANY SECRETS: OVERCLASSIFICATION AS A BARRIER TO CRITICAL INFORMATION SHARING

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS AND INTERNATIONAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

AUGUST 24, 2004

Serial No. 108–263

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

98–291 PDF WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
DOUG OSE, California
RON LEWIS, Kentucky
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
NATHAN DEAL, Georgia
CANDICE S. MILLER, Michigan
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio
JOHN R. CARTER, Texas
MARSHA BLACKBURN, Tennessee
PATRICK J. TIBERI, Ohio
KATHERINE HARRIS, Florida

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. "DUTCH" RUPPERSBERGER, Maryland
ELEANOR HOLMES NORTON, District of Columbia
JIM COOPER, Tennessee
BETTY MCCOLLUM, Minnesota

BERNARD SANDERS, Vermont (Independent)

MELISSA WOJCIAK, *Staff Director*
DAVID MARIN, *Deputy Staff Director/Communications Director*
ROB BORDEN, *Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHIL BARNETT, *Minority Chief of Staff/Chief Counsel*

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS AND INTERNATIONAL RELATIONS

CHRISTOPHER SHAYS, Connecticut, *Chairman*

MICHAEL R. TURNER, Ohio
DAN BURTON, Indiana
STEVEN C. LATOURETTE, Ohio
RON LEWIS, Kentucky
TODD RUSSELL PLATTS, Pennsylvania
ADAM H. PUTNAM, Florida
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
TIM MURPHY, Pennsylvania
KATHERINE HARRIS, Florida

DENNIS J. KUCINICH, Ohio
TOM LANTOS, California
BERNARD SANDERS, Vermont
STEPHEN F. LYNCH, Massachusetts
CAROLYN B. MALONEY, New York
LINDA T. SANCHEZ, California
C.A. "DUTCH" RUPPERSBERGER, Maryland
JOHN F. TIERNEY, Massachusetts
DIANE E. WATSON, California

EX OFFICIO

TOM DAVIS, Virginia
HENRY A. WAXMAN, California

LAWRENCE J. HALLORAN, *Staff Director and Counsel*
ROBERT A. BRIGGS, *Clerk*
ANDREW SU, *Minority Professional Staff Member*

CONTENTS

TOO MANY SECRETS: OVERCLASSIFICATION AS A BARRIER TO CRITICAL INFORMATION SHARING

TUESDAY, AUGUST 24, 2004

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS AND INTERNATIONAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:05 a.m., in room 2154, Rayburn House Office Building, Hon. Christopher Shays (chairman of the subcommittee) presiding.

Present: Representatives Shays, Platts, Kucinich, Ruppersberger, and Tierney.

Staff present: Lawence Halloran, staff director and counsel; Thomas Costa, professional staff member; Jean Gosa, minority assistant clerk; and Andrew Su, minority professional staff member.

Mr. SHAYS. A quorum being present, the Subcommittee on National Security, Emerging Threats, and International Relations hearing entitled, "Too Many Secrets: Overclassification is a Barrier to Critical Information Sharing," is called to order.

An old maxim of military strategy warns, "He who protects everything, protects nothing."

Nevertheless, the United States today attempts to shield an immense and growing body of secrets using an incomprehensibly complex system of classifications and safeguard requirements. As a result, no one can say with any degree of certainty how much is classified, how much needs to be declassified, or whether the Nation's real secrets can be adequately protected in a system so bloated, it often does not distinguish between the critically important and the economically irrelevant.

This much we know: There are too many secrets. Soon after President Franklin Roosevelt's first executive order on classification in 1940, the propensity to overclassify was noted. Since then, a long and distinguished list of committees and commissions has studied the problem. They all found it impossible to quantify the extent of overclassification because no one even knows the full scope of the Federal Government's classified holding at any given time. Some estimate 10 percent of current secrets should never have been classified. Others put the extent of overclassification as high as 90 percent.

During the cold war, facing a monolithic foe determined to penetrate our national secrets, overclassification may have provided a

needed security buffer. But the risk/benefit calculation has changed dramatically. Against a stateless, adaptable enemy, we dare not rely on organizational stovepipes to conclude, in advance, who should have access to one piece of an emerging mosaic. Connecting the dots is now a team sport. The cold war paradigm of "need to know" must give way to the modern strategic imperative, "the need to share."

The National Commission on Terrorist Attacks Upon the United States, referred to as the 9/11 Commission, concluded that, "Current security requirements nurture overclassification and excess compartmentation of information among agencies. Each agency's incentive structure opposes sharing, with risks—criminal, civil, and internal administrative sanctions—but few rewards for sharing information. No one has to pay the long-term costs of overclassifying information, though these costs—even in literal financial terms—are substantial."

The National Archives' Information Security Oversight Office, ISOO, reported that in 2003, more than 14 million documents were classified by the 3,978 Federal officials authorized to do so. They classified 8 percent more information than the year before. But recently declassified documents confirm the elaborate and costly security applied to some information is simply not worth the effort or expense. A former dictator's cocktail preferences and a facetious plot against Santa Claus are not threats to national security in the public domain, yet both were classified.

The most recent ISOO report correctly concludes "allowing information that will not cause damage to national security to remain in the classification system or to enter that system in the first instance, places all classified information at needless increased risk."

Current classification practices are highly subjective, inconsistent and susceptible to abuse. One agency protects what another releases. Rampant overclassification often confuses national security with bureaucratic, political or a diplomatic convenience.

The dangerous, if natural, tendency to hide embarrassing or inconvenient facts can mask vulnerabilities and only keeps critical information from the American people. The terrorists know their plans. Fewer people classifying fewer secrets would better protects national security by focussing safeguards on truly sensitive information, while allowing far wider dissemination of the facts and analysis, the 9/11 Commission says, must be shared.

Any discussion of intelligence reform must include a new approach to classification, one that sheds cold war shackles and serves the strategic needs to share information. Our witnesses this morning bring impressive experience and insight to this important issue and we look forward to their testimony. I welcome each of them.

At this time, the Chair would recognize the ranking member of the committee, Mr. Kucinich.

[The prepared statement of Hon. Christopher Shays follows:]

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS,
AND INTERNATIONAL RELATIONS
Christopher Shays, Connecticut
Chairman
Room B-372 Rayburn Building
Washington, D.C. 20515
Tel: 202 225-2548
Fax: 202 225-2382

Statement of Rep. Christopher Shays
August 24, 2004

An old maxim of military strategy warns, "he who protects everything protects nothing."

Nevertheless, the United States today attempts to shield an immense, and growing, body of secrets using an incomprehensibly complex system of classifications and safeguard requirements. As a result, no one can say with any degree of certainty how much is classified, how much needs to be declassified or whether the nation's real secrets can be adequately protected in a system so bloated it often does not distinguish between the critically important and the comically irrelevant.

This much we know: there are too many secrets. Soon after President Franklin Roosevelt's first Executive Order on classification in 1940, the propensity to overclassify was noted. Since then, a long and distinguished list of committees and commissions has studied the problem. They all found it impossible to quantify the extent of overclassification because no one even knows the full scope the federal government's classified holdings at any given time. Some estimate ten percent of current secrets should never have been classified. Others put the extent of overclassification as high as ninety percent.

During the Cold War, facing a monolithic foe determined to penetrate our national secrets, overclassification may have provided a needed security buffer. But the risk/benefit calculation has changed dramatically. Against a stateless, adaptable enemy, we dare not rely on organizational stovepipes to conclude, in advance, who should have access to one piece of an emerging mosaic. Connecting the dots is now a team sport. The Cold War paradigm of "need to know" must give way to the modern strategic imperative – the need to share.

The National Commission on Terrorist Attacks Upon the United States ("the 9/11 Commission) concluded that:

> "Current security requirements nurture overclassification and excessive compartmentation of information among agencies. Each agency's incentive structure opposes sharing, with risks (criminal, civil, and internal administrative sanctions) but few rewards for sharing information. No one has to pay the long-term costs of over-classifying information, though these costs—even in literal financial terms— are substantial."

The National Archives' Information Security Oversight Office (ISOO) reported that in 2003 more than 14 million documents were classified by the 3978 federal officials authorized to do so. They classified eight percent more information than the year before.

But recently declassified documents confirm the elaborate and costly security applied to much information is simply not worth the effort or expense. A former dictator's cocktail preferences and a facetious plot against Santa Claus are no threat to national security in the public domain, yet both were classified. The most recent ISOO report correctly concludes, "Allowing information that will not cause damage to national security to remain in the classification system, or to enter that system in the first instance, places all classified information at needless increased risk."

Current classification practices are highly subjective, inconsistent and susceptible to abuse. One agency protects what another releases. Rampant overclassification often confuses national security with bureaucratic, political or diplomatic convenience.

The dangerous, if natural, tendency to hide embarrassing or inconvenient facts can mask vulnerabilities and only keeps critical information from the American people. The terrorists know their plans. Fewer people classifying fewer secrets would better protect national security by focusing safeguards on truly sensitive information, while allowing far wider dissemination of the facts and analysis the 9/11 Commission says must be shared.

Any discussion of intelligence reform must include a new approach to classification, one that sheds Cold War shackles and serves the strategic need to share information. Our witnesses this morning bring impressive experience and insight to this important issue, and we look forward to their testimony.

Welcome.

Mr. KUCINICH. Thank you very much, Mr. Chairman. Thank you for calling this very important hearing. I want to thank the witnesses for their attendance and acknowledge the presence of my colleagues.

The overclassification of Federal materials is a growing problem, a problem that has been highlighted once again in the final report of the 9/11 Commission. Overclassification has serious fiscal costs. It also reduces the accountability and reduces our security. But the real problem is not the quantity of materials classified and declassified. Thereal problem, I would submit, is the systemic and reflexive secrecy rampant throughout officials in this administration.

But I have to say, as the witnesses certainly know, this problem of overclassification, of secrecy, has been a problem throughout the history of this country. And in a book, Mr. Chairman, which you may be familiar with, Chalmers Johnson, who is a scholar, wrote a book about secrecy and his relationship to what he calls "militarism secrecy and the end of the Republic." The book is called "The Sorrows of Empire." And he was also the person who is the author of an a book called "Blow Back," which talks about the consequences of the U.S. foreign policy on what happens here at home.

This book really makes the connections on how secrecy undermines our country. And in a culture of increased military spending, together with the secrecy, it makes it very difficult for taxpayers to have any idea what is going on and how their dollars are being spent; and it really reflects on the priorities of the country.

This problem of secrecy is also something we have to deal with as Members of Congress. How many so-called "secret briefings" has the Congress had over the past few years where we were just fed misinformation for the purposes of being able to gain support in Congress for things that people otherwise would not have supported. But the meetings were kept secret and that is a way that you stop a discussion in a free society.

Now, the current situation with this administration—instead of making information available or sharing information, this administration reversed a trend started in the Clinton administration, a trend toward openness, the Clinton Executive Order 2958. Under this order there is a presumption against classification, and this presumption was used in case of doubt, and where there was doubt about the appropriate level of classification, the order specified that the material be classified at the lower level. An interagency security classification appeals panel was established and historical records were declassified at record rates and on a timely automated schedule.

In contrast, the current administration has dramatically increased the volume of Federal materials concealed from the American people. Executive Order 13292, issued in March 2003, 18 months after September 11, permitted officials to classify information when there was doubt whether or not to do so, allowed officials to classify information at the more restrictive level when there was a question as to the appropriate level.

The order also delayed and weakened the system of automatic declassification established under the Clinton executive order and underutilized the appeals panel. As a result, as has been noted ear-

lier, a record 14 million classification actions were reported last year, costing U.S. taxpayers an all-time high of $6.5 billion.

The total number of pages declassified by this administration was the lowest in the last 10 years, annual FOIA requests, Freedom of Information Act requests, have become more tightly controlled, surpassing the $3 million mark last year for the first time in history and costing the government $325 million.

Secrecy is on the rise throughout the administration. Officials at the Environmental Protection Agency, the Department of Agriculture, the Department of Health and Human Services now have been granted classification authority, while the Office of the Vice President has become exempt from certain mandatory declassification reviews.

The FCC, Federal Communications Commission, recently stated that outage reports from wireless, line, cable and telecom providers would be protected from public disclosure because of "increasing concern about homeland security and national defense."

In addition, the Nuclear Regulatory Commission recently decided that information about the physical security of nuclear facilities would no longer be publicly available or updated on the agency's Web site, though this information would be critical for public health and safety. And I want to say that I am pleased this subcommittee will be holding hearings on this issue of nuclear plant security in the coming weeks.

Information seems to be arbitrarily and unnecessarily classified. Last week, the American Civil Liberties Union released court documents showing that the Justice Department tried to file secret affidavits in two civil court cases challenging the USA Patriot Act. These affidavits can only be viewed by the judge and would not be seen by the public or even the plaintiffs.

The attack on the civil liberties of U.S. citizens now includes this new tactic. The Justice Department even attempted to redact harmless information, such as a quotation from a 1972 Supreme Court ruling, and general descriptions of a company and the fact that it did consulting work.

Even more egregiously, we have seen the declassification used as an excuse to avoid embarrassment to the administration. The Senate Intelligence Committee's report on prewar intelligence concerning the Iraqi WMD program was redacted. The entire report of Major General Antonio Taguba, detailing the mistreatment of Iraqi prisoners at Abu Ghraib prison, was classified, though it did not reveal intelligence sources or methods.

Even in this committee, we saw how the Pentagon retroactively classified sections of a report critical of the proposed national missile defense plan by Philip Coyle, Director of the Department of Defense Office of Operational Test and Evaluation. The information in the report which had been disclosed and widely disseminated was subsequently withheld from Congress for 8 months. The Pentagon then marked a report "For Official Use Only" and classified the 50 specific recommendations stated in Mr. Coyle's report so it could not be released to the public for scrutiny.

The final report of the 9/11 Commission confirms what many of us already know too well. The Bush administration's excessive use of classification, delay in declassifying Federal materials and en-

croachments on the civil rights of individuals are antithetical to democratic principle; and it is our responsibility, as Congress, to provide effective checks and balances, which is really the purpose of this committee.

Thank you, Mr. Shays.

[The prepared statement of Hon. Dennis J. Kucinich follows:]

Statement of Rep. Dennis J. Kucinich
Ranking Minority Member
House Subcommittee on National Security, Emerging Threats, and International Relations

Hearing on "Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing"

August 24, 2004

Good morning. The overclassification of federal materials is a growing problem, a problem that has been highlighted once again by the final report of the 9/11 Commission. Overclassification has serious fiscal costs. It reduces accountability, and reduces our security. But the real problem is not the quantity of materials classified and declassified, it is the systemic and reflexive secrecy rampant throughout officials in the current Administration.

Instead of making information available or sharing information, the current Administration has reversed the trend towards openness started under the Clinton Administration.

Under Clinton Executive Order 2958, a presumption against classification was used in cases of doubt, and when there was

doubt about the appropriate level of classification, the order specified that the material be classified at the lower level. An interagency Security Classification Appeals Panel was established, and historical records were declassified at record rates and on a timely, automated schedule.

In contrast, the Bush Administration has dramatically increased the volume of federal materials concealed from the American people. Bush executive order 13292 issued in March 2003 (18 months after the September 11, 2001 attacks) permitted officials to classify information when there was doubt whether or not to do so, and allowed officials to classify information at the more restrictive level when there was a question as to the appropriate level. The order also delayed and weakened the system of automatic declassification established under the Clinton executive order and underutilized the appeals panel.

As a result, a record 14 million classification actions were reported last year, costing U.S. taxpayers an all time high of $6.5 billion. The total number of pages declassified by this

Administration was the lowest in the last ten years. Annual FOIA requests have also become more tightly controlled, surpassing the 3 million mark last year for the first time in history, and costing the government $325 million.

Secrecy is on the rise throughout this Administration. Officials at the Environmental Protection Agency, Department of Agriculture, and Department of Health and Human Services now have been granted classification authority, while the Office of Vice President has become exempt from certain mandatory declassification reviews.

The FCC recently stated that outage reports from wireless, line, cable, and telecom providers would be protected from public disclosure because of "increasing concern about homeland security and national defense."

In addition, the Nuclear Regulatory Commission recently decided that information about the physical security of nuclear facilities would no longer be publicly available or updated on the agency's web site, though this information could be critical for

public health and safety. I am pleased that this Subcommittee will be holding hearings on nuclear plant security in the coming weeks.

Information seems to be arbitrarily and unnecessarily classified. Last week, the American Civil Liberties Union released court documents showing that the Justice Department tried to file secret affidavits in two civil court cases challenging the USA Patriot Act. These affidavits can only be viewed by the judge, and would not be seen by the public or even the plaintiffs. The attack on the civil liberties of U.S. citizens now includes this new tactic. The Justice Department even attempted to redact harmless information, such as a quotation from a 1972 Supreme Court ruling, and general descriptions of a company and the fact that it did consulting work.

Even more egregiously, we have seen declassification used as an excuse to avoid embarrassment to the Administration. The Senate Intelligence Committee's report on pre-war intelligence concerning the Iraqi WMD program was redacted. The entire report of Maj. Gen. Antonio Taguba detailing the mistreatment of

Iraqi prisoners at Abu Ghraib prison was classified, though it did not reveal intelligence sources or methods.

Even in this committee, we saw how the Pentagon retroactively classified sections of a critical report of the proposed national missile defense plan by Philip Coyle, the director of the DOD Office of Operational Test and Evaluation. The information in the report, which had been disclosed and widely disseminated, was subsequently withheld from Congress for eight months. The Pentagon then marked the report "For Official Use Only" and classified the 50 specific recommendations stated in the Mr. Coyle's report, so that it could not released to the public for scrutiny.

The final report of the 9/11 Commission confirms what many of us already know too well. This Administration is the most secretive in history. The Bush Administration's excessive use of classification, delay in declassifying federal materials, and encroachments on the civil rights of individuals is beyond comparison. It is our duty to question why that is the case – is this

Administration keeping secrets from our enemies, or is it keeping secrets from American citizens?

Mr. SHAYS. I thank the gentleman.

At this time the Chair would recognize Mr. Tierney.

Mr. TIERNEY. Thank you, Mr. Chairman. Mr. Chairman, I join with members of the public and Members of Congress and, of course, the September 11 families in hoping that Congress will act swiftly to implement the unanimous bipartisan recommendation of the 9/11 Commission Report.

I must say that as we address today's issue, the Commission's strong and unequivocal recommendations that the executive branch move from treating information on a "need to know" to a "need to share" basis, I am uncertain that this transformation can occur within an administration that has overemphasized classification at the expense of congressional oversight and, in some cases, at the expense of common sense.

I know during the last administration, in 1995, the President reset previous default settings, directing classifiers not to shield information of doubtful value and to classify information at the lowest rather than the highest possible level. Reclassification was prohibited if the material had otherwise been properly put in the public domain.

Under this President Bush, his executive order reverts to a "when it doubt, classify" standard, expands classification authorities and categories, and postpones automatic declassification on some records.

Now, this leads us here today to ask the witnesses, how can the administration convince a skeptical public that the administration is committed to changing this culture when, even as we speak, they are continuing to classify, in some cases retroactively, information pertaining to our national defense.

One key example was mentioned briefly by Mr. Kucinich, and it has to do with missile defense. I happen to have a longer history with this issue, and so I want to take a moment to recount it. And the chairman has shared this history.

In the context of the 9/11 Commission Report, the most immediate threat is not an incoming intercontinental ballistic missile, but an act of terror, some biological or chemical agent introduced in this country, or a dirty bomb delivered in a suitcase. Even our own intelligence agencies prioritize threats in this manner. So the public has the right to ask, why is this administration spending more than $10 billion per year on a national missile defense system instead of protecting our ports, equipping the Coast Guard or our local first responders, protecting chemical facilities, our nuclear reactors, and so on down the line—the many things that need to be done, which are underfunded seriously in the President's budget and in the majority's budget.

The public has the right to an answer.

Do experts and security personnel think this system will work? The answer is "no." Forty-nine previous generals and admirals and other higher retired military individuals speak out against deployment at this point in time. In a letter to the President, they clearly set out, "As you have said, Mr. President, our highest priority is to prevent terrorists from acquiring and employing weapons of mass destruction. We agree. We therefore recommend, as the militarily responsible course of action, that you postpone operation and

deployment of the expensive and untested GMD system and transfer the associated funding to accelerated programs to secure the multitude of facilities containing nuclear weapons and materials and to protect our ports and borders against terrorists who may attempt to smuggle weapons of mass destruction into the United States."

In addition, 31 former government officials called the missile defense deployment a "sham." These are officials who worked for Presidents Eisenhower, Kennedy, Johnson, Nixon, Carter, Reagan, George H.W. Bush, and Clinton, and argued that the missile defense system planned for rollout in September will provide no real defense, as they called it a "sham." The officials worked at the Pentagon, the Department of State, the National Security Council, the Office of Management and Budget, the Arms Control and Disarmament Agency; and their letter accused the administration of rushing a program into a field that is largely untested and missing major components.

The fact of the matter is, the public should know whether or not this President, for political purposes, is satisfying his ideological extremists by deploying an unproven, inadequately tested system; and in fact, is he living in the past instead of addressing the concerns that we have in the 21st century. But instead of allowing for a public examination, this administration has classified relevant critical reports and facts, even reclassifying some that have been in the public domain for as much as 4 or 5 years for what can be argued as "political purposes."

I will not go through the long rendition, Mr. Chairman, of the many letters we have, but starting back in September 8, 2000, this subcommittee held a hearing with the then-Director of Operational Tests and Evaluation, the Pentagon's own person, Phil Coyle, who testified about the inadequacies of the missile defense system. And at that time I asked the subcommittee, and the subcommittee agreed without objection, to enter his report detailing 50 recommendations for how this system should be tested. And we put that in the public record.

What occurred after that was a pattern of stonewalling and repeated resistance from the Department of Defense that lasted over 8 months. Finally, on May 31, 2001 the Coyle report was delivered to Congress. As Mr. Kucinich mentioned, it was first marked "For Official Use Only," but when challenged, the Department of Defense was unable to respond to what that category meant and certainly did not indicate that it was classified in any sense.

Finally, Chairman Shays took the lead and decided to make this information available to the public on June 2001. It was on the Web site. It was in public documents. And since that point in time, we have had numerous hearings in this committee. We have had testimony from experts. We have had poster boards set up with the information on it. We have had it on our own Web sites.

And finally, I asked the General Accounting Office to prepare a report to tell us in September 2004 what would the condition of deployment be, especially with respect to the 50 issues by Mr. Coyle. After fighting for an inordinate period of time, the General Accounting Office was finally able to issue a report. It no sooner hit my desk than this administration classified that report. You can

imagine for yourself whether it was a favorable report to their position or unfavorable.

Not satisfied with that, we asked them to go back and look over every line and tell us what was classified and was not. Having done that, they issued a classified report and an unclassified report. The unclassified report, in my estimation was damning. You can imagine what the classified report was. But then the administration took the additional step of going back in, reclassifying all the previously open, available information upon which those reports were based, none of them previously having been classified, all of the information having been in the public domain for some 4 years.

You can answer the question better than I can, but why should this administration be trusted with the recommendation of the September 11 Commission to move toward a culture of "need to share" as opposed to "need to know?"

But it is not all about the missile defense system. There is a disturbing pattern in this administration of using secrecy as a means to defend or advance their political purposes and policies.

When confronted with allegations that the Energy Task Force, which the Vice President convened, was predominantly comprised of industry members who would be inclined to favor the status quo energy policy in this country, the Bush administration refused to come clean and disclose participants of the task force, arguing that such inquiries into Federal agencies are off limits to the courts, the Congress, and thus, the American people.

In June 2003, when the Environmental Protection Agency released a report on the state of the environment, the detailed assessment of climate change, which among other things was to conclude that carbon dioxide emissions are contributing to global warming, was deleted by the White House and replaced with language that was deliberately vague and disingenuous about the scientific causes of global warming.

After hearing the compelling evidence of defective tires on certain automobiles and the tragedies that ensued on America's roads, Congress passed a law making certain that auto safety data be made available to the public. But this administration's National Highway Traffic Administration has decided that such information regarding unsafe automobiles which may be detrimental to their companies will remain secret.

And now, according to Friday's Washington Post, the Department of Justice in its court battle with the American Civil Liberties Union over portions of the Patriot Act has attempted to rely on secret evidence. As Mr. Kucinich also mentioned, one aspect of that was inessential censoring a dozen seemingly innocuous passages on national security grounds, including an attempt to redact a quotation from a 1972 Supreme Court ruling that simply said, "The danger to political dissent is acute where the government attempts to act under so vague a concept as the power to protect domestic security. Given the difficulty of defining the domestic security interests, the danger of abuse and acting to protect that interest become apparent."

Now, there is a dangerous statement if I ever heard one. But this administration's Department of Justice thought that had to be redacted from a court proceeding.

This reliance on classification and withholding of information does not just prevent transparency and accountability in public policymaking. It is an act that is fundamentally opposed to the public; it is opposed to their health, to their civil liberties, to their consumer interests, and most importantly, to their safety.

How can we trust that this administration with this record will commit itself to implementing the 9/11 Commission's recommendation that we have more transparency, that we move to a culture of sharing, a "need to share" versus a "need to know"? At a time when it is so important that we put our resources where the dangers appear most and not on some ideological extreme program that is unproven and untested, hiding the facts is not doing this country any service. And we have to take the recommendations of the 9/11 Commission seriously.

I hope these hearings, Mr. Chairman, will move us in that direction of classifying only what needs to be classified and sharing the rest, so that the American people can make the right choices and the right priorities for our safety. Thank you.

Mr. SHAYS. I thank the gentleman for his statement.

At this time the Chair would recognize Mr. Ruppersberger, who serves on the House Intelligence Committee.

Mr. RUPPERSBERGER. Mr. Chairman, I want to thank you. We have a tremendous opportunity at this time in our history to provide for national security as a result of what happened on September 11. I want to first praise the Commission and all of those people involved, including the families of those who died in the September 11 incident.

At this point, it is very, very important that we deal with this issue in a nonpartisan way. And it is important that we also understand that there are different elements we have to deal with as far as the 9/11 Commission's report.

First, it is extremely important that we do have one person that can hold all the intelligence communities accountable. We have to make sure that the intelligence communities, all of them, including the military, the DOD, CIA, NSA, all the intelligence communities, work as a team and that they integrate the information. We can be extremely sophisticated in our intelligence community, but if we do not get to the bottom line and do what needs to be done and get the right information to the right people, we will not be successful in what is our goal of national security.

Now, the issue we are dealing with today is overclassification as a barrier to critical information. I think it is extremely important that we deal with this issue. Just one aspect of this overclassification is also the barrier in getting people cleared and how ridiculous it is. I have a Federal Times, August 16, "482,000 Wait For Clearance, Backlog of Security Checks Holds Up Work, Wastes Billions of Dollars."

Now, one of the American intelligence community's greatest problems is the cult of classification in which information, both rare and commonplace, is a safeguard with equal zeal. Both cases also illustrate the intense political pressures on intelligence and

counterintelligence agencies, diluting the value of the Nation's intelligence. These are parts of our system that are broken, the ones that no one in Washington wants to talk about, but we are going to have to deal with to fix this testimony.

There is certainly vital information that must be protected from foreign espionage. These secrets worth saving should be held closely. Far too much effort is being wasted protecting nonsecrets which allows vital secrets to slip through.

In Washington, classification has led to sort of a game, creating those "in the know" and those who are "not in the know." This game heightens the power of bureaucrats, but so much is classified that it is impossible for people with security clearances to know what is derived from a spy satellite and what is plucked out of the newspaper, which is considered open source.

So what is a secret? Nuclear secrets should be kept secret. The names of U.S. agents in other countries must be kept secret. Operation capabilities of U.S. weapons should be kept secret. Unlike today's situation, a secret requires that there not be the slightest hint that even a secret exists. To do that, the government would need to follow just a few simple rules instead of the myriad of complexities it has erected. And whether it is a Democratic administration, or a Republican, there is not consistency in what we do as far as this classification is concerned. And we need consistency. We need standards.

First, there must be few secrets. Unless you are willing to stash people, it is easiest to keep a small number of secrets. Second, give secrets to fewer people. The idea of hundreds of thousands of people wandering around with secrets is absurd. Do not use access to classified materials as a justification for doing background checks on military officers. Just do background checks.

Do not classify as secret that which is in the New York Times and on the Internet. Do not use secrecy as a shield to protect idiotic political and policy decisions.

I am looking forward to hearing what your recommendations would be to deal with this very important issue. It is a strong component of what we need to deal with to provide the best national security for our country.

Intelligence clearly is the best defense against terrorism, but we need to get our system right, consistent, and focused. Thank you.

Mr. SHAYS. I thank the gentleman, especially your comments, given that you do serve on the Intelligence Committee. I would just say, I appreciate the gentleman breaking a family vacation to be here.

I have the opportunity to ask the first questions. I am going to defer to you to start off, and then we'll go to Mr. Kucinich, Mr. Tierney and myself. I ask unanimous consent that all members of the subcommittee be permitted to place an opening statement in the record and that the record remain open for 3 days for that purpose.

Without objection, so ordered.

I ask further unanimous consent that all witnesses be permitted to include their written statement in the record.

Without objection, so ordered.

This is a fairly big document that I have shown the ranking member. It's entitled, "Dubious Secrets: A Briefing Book of Overclassified Documents," prepared by the National Security Archive, George Washington University. I am going to ask that it be submitted into the record.

Without, objection.

[NOTE.—The report entitled, "Dubious Secrets: A Briefing Book of Overclassified Documents," may be found in subcommittee files. A copy of the title page follows:]

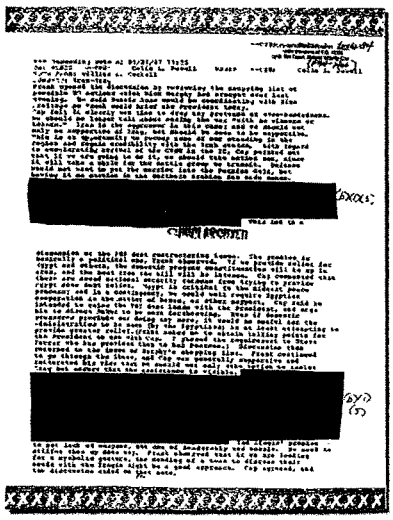
DUBIOUS SECRETS:
A BRIEFING BOOK OF OVERCLASSIFIED DOCUMENTS

Prepared by the National Security Archive,
George Washington University,
Thomas S. Blanton, Executive Director

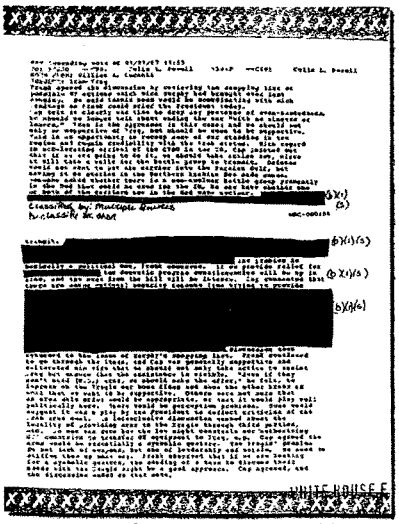
For the U.S. House of Representatives,
Committee on Government Reform,
Subcommittee on National Security, Emerging Threats, and International Relations, Oversight Hearing:
"Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing"

August 24, 2004, Rayburn Building Room 2154, Washington D.C.

White House e-mail to Colin L. Powell, January 21, 1987 (see Document 18)



Released June 6, 1994



Released June 15, 1994

Mr. SHAYS. I want to just note that the George Washington Archive maintains a body of documentation demonstrating the inconsistency and the arbitrariness of many classified decisions. They find documents released by one agency classified in whole or in part by another, and they track a declassification process they find to be extraordinarily slow and litigious.

Without objection, we will put that in the record.

At this time, I recognize our witnesses. We have Mr. William Leonard, Director, Information Security Oversight Office, National Archives and Records Administration. We have Carol Haave, Deputy Under Secretary of Defense for Counterintelligence and Security, Department of Defense; Mr. Steven Aftergood, Federation of American Scientists; and Mr. William P. Crowell, the Markle Foundation Task Force on National Security in the Information Age.

We truly have four experts on this issue. It is not an easy issue to deal with, and given that we have one panel, we will have the 5 minutes that you may speak; you can trip over a little bit. I'd just as soon you not take another 5 minutes but you have that right. Then we will go to 10 minutes of questioning.

At this time, we will swear in our witnesses. Is there anyone else that has accompanied you that might provide information so they can stand and be sworn in at this time.

Is there anyone else?

No one else.

[Witnesses sworn.]

Mr. SHAYS. Note for the record our witnesses have responded in the affirmative.

At this time we will begin with you, Mr. Leonard. Thank you for being here.

STATEMENTS OF J. WILLIAM LEONARD, DIRECTOR, INFORMATION SECURITY OVERSIGHT OFFICE, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION; CAROL A. HAAVE, DEPUTY UNDER SECRETARY OF DEFENSE, COUNTERINTELLIGENCE AND SECURITY, U.S. DEPARTMENT OF DEFENSE; STEVEN AFTERGOOD, FEDERATION OF CONCERNED SCIENTISTS; AND WILLIAM P. CROWELL, THE MARKLE FOUNDATION TASK FORCE ON NATIONAL SECURITY IN THE INFORMATION AGE

Mr. LEONARD. Mr. Chairman, Mr. Kucinich, members of the panel. I wish to thank you for holding this hearing on security classification and declassification issues. As Director of the Information Security Oversight Office, I am responsible to the President for overseeing the governmentwide classification program within both government and industry.

Executive Order 12958, as amended, sets forth the basic framework by which executive branch agencies classify national security information. Pursuant to his constitutional authority in this order, the President authorizes a limited number of individuals to apply classification to certain national security-related information. While the order is clear that the employment of classification is based in large part upon the judgment of an original classifying authority, in delegating classification authority, the President has established

clear parameters for its use and certain burdens that must be satisfied.

Classification authority is not without limits. The President has spelled out some very clear prohibitions with respect to the use of classification. Specifically, in no case can information be classified in order to conceal violations of law or prevent embarrassment to a person, an organization, or an agency. Unfortunately, there have been instances giving the impression that information has been classified in violation of the order. In each case I am aware of, I have found that this often arises due to lack of proactive oversight within agencies or a lack of effective training and awareness provided to some cleared personnel.

I believe that the overall policy for security classification as set forth in the current executive order is fundamentally sound. While I and others, including the 9/11 Commission, have advocated revisions to basic concepts such as the "need-to-know" principle, the order as currently configured is replete with measures to ensure the classification system's continued effectiveness. Many agencies are excelling at fulfilling these requirements; others are not.

It is no secret that the government classifies too much information. Many senior officials will candidly acknowledge the problem of excessive classification. This is supported in part by agency input to my office that indicates that overall classification activity is up over the past several years.

What I find most troubling, however, is that some individual agencies have no idea how much information they generate is classified, whether the overall quantity is increasing or decreasing, what the explanations are for such changes, which elements within their organization are most responsible for the changes, and most importantly of all, whether the changes are appropriate.

The identification of baseline information such as this is essential for agencies to be able to ascertain the effectiveness of the classification efforts.

My current concerns extend to the area of declassification as well. It's disappointing to note that declassification activity has been down for the past several years. In some quarters, when it comes to classification in times of national security challenges, when available resources are distracted elsewhere, the approach toward classification and declassification can be to err on the side of caution. Yet the classification system is too important and the consequences resulting from improper implementation too severe to allow error to be the part of any implementation strategy.

Both too little and too much classification is not an option. Too much classification unnecessarily impedes effective information sharing. And inappropriate classification undermines the integrity of the entire process. Too little classification can subject our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations to potential harm.

Proactive oversight by agencies of their security classification program and involvement by senior leadership is crucial.

The security classification system is permissive, not prescriptive. It identifies what information can be classified, not what information must be classified. The decision to classify information or not is ultimately the prerogative of an agency and its original classi-

fication authorities. The problem, however, with all due apologiesto John Donne, is that no agency is an island.

The exercise of agency prerogative to classify certain information has ripple effects throughout the entire executive branch, as well as the Nation as a whole. It can serve as an impediment to sharing information with another agency or with the public who have a genuine need to know about the information.

The 9/11 Commission has recommended that information procedures should provide incentives for sharing to restore a better balance between security and shared knowledge. The administration is currently developing guidelines and regulations to improve information sharing both among Federal departments and agencies and between the Federal Government and State and local entities.

On August 2 of this year, President Bush announced that he will be issuing a directive requiring all relevant agencies to complete the task of adopting common data bases and procedures so that intelligence and homeland security information can be shared and searched effectively, consistent with privacy and civil liberties.

I thank you for inviting me here today Mr. Chairman. I will be happy to answer any questions you and the committee may have.

Mr. SHAYS. Thank you, Mr. Leonard.

[The prepared statement of Mr. Leonard follows:]

FORMAL STATEMENT

J. William Leonard
Director, Information Security Oversight Office
National Archives and Records Administration
before the
Committee on Government Reform
Subcommittee on National Security, Emerging Threats,
and International Relations
U.S. House of Representatives
August 24, 2004

Chairman Shays, Mr. Kucinich, and members of the Subcommittee, I wish to thank you for holding this hearing on security classification and declassification issues as well as for inviting me to testify today. As Director of the Information Security Oversight Office (ISOO), I am responsible to the President for overseeing the Government-wide security classification program in both Government and industry. An administrative component of the National Archives and Records Administration, my office receives policy and program guidance from the National Security Council. Our authority is found in two Executive orders, Executive Order 12958, as amended, "Classified National Security Information," and Executive Order 12829, as amended, "National Industrial Security Program."

It is Executive Order 12958 that sets forth the basic framework by which executive branch agencies classify national security information. Pursuant to his constitutional authority, in this Order the President authorizes a limited number of officials to apply classification to certain national security related information. While the Order is clear that the employment of classification is an inherently discretionary act, based in large part upon the judgment of an original classifying authority, in delegating classification authority the President has established clear parameters for its use and certain burdens that must be satisfied. Specifically, every act of classifying information must be able to trace its origin to an explicit decision by a responsible official who has been expressly delegated original classification authority. In addition, when required, the original classification authority must be able to identify or describe the damage to national security that would arise if the information were subject to unauthorized disclosure. Furthermore, the information must be owned by, produced by or for, or under the control of the United States Government; and finally, it must fall into one or more of the categories of information specifically provided for in the Order.[1]

It is important to recognize that classification authority is not without limits. The President has spelled out some very clear prohibitions with respect to the use of

[1] Pursuant to § 1.4 of the Order, information shall not be considered for classification unless it concerns: (a) military plans, weapons systems, or operations; (b) foreign government information; (c) intelligence activities (including special activities), intelligence sources or methods, or cryptology; (d) foreign relations or foreign activities of the United States, including confidential sources; (e) scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism; (f) United States Government programs for safeguarding nuclear materials or facilities; (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or (h) weapons of mass destruction.

classification. Specifically, in no case can information be classified in order to conceal violations of law or to prevent embarrassment to a person, organization or agency. Unfortunately, there have been instances giving the impression that information has been classified in violation of the Order. In each case I am aware of, I do not believe it arose out of mal intent on the part of any individual. Rather, it often arises due to a lack of proactive oversight within agencies and a lack of effective training and awareness provided to some cleared personnel. In every instance that comes to our attention, we work with the agencies involved in order to ensure that adequate corrective action is taken.

I believe that the overall policy for security classification as set forth in the current Executive order is fundamentally sound. While I and others, to include the "9/11 Commission," have advocated revisions to basic concepts such as the "need-to-know" principle, the Order as currently configured is replete with measures to ensure the classification system's continued effectiveness. For example, each agency must appoint a senior official to oversee its program, promulgate internal regulations, establish and maintain security education and training programs, as well as an ongoing self-inspection program, and commit the resources necessary to ensure effective implementation of the program. Many agencies are excelling at fulfilling these requirements; others are not.

For example, it is no secret that the Government classifies too much information. In my over 30 years of experience in security and counterintelligence matters, I have observed that many senior officials will candidly acknowledge the problem of excessive classification, although oftentimes the observation is made with respect to the activities of agencies other than their own. The potential issue of excessive classification is supported, in part, by agency input to my office that indicates that overall classification activity is up over the past several years. For example, based upon information furnished our office, the total number of classification decisions increased from 9 million in FY 2001 to 11 million in FY 2002 and 14 million in FY 2003. However, these increases do not necessarily indicate a penchant for secrecy on the part of Federal agencies — they also reflect how busy these agencies are. Since 9/11, and especially with respect to the Global War on Terrorism and the Iraq War, more and more agency operations have been working on a 24/7 basis — which will naturally increase the activities' overall output, to include the number of classification decisions.

That said, I believe a more meaningful metric is the number of original classification decisions made within agencies (i.e., the initial determination by an authorized classifier that specific information requires protection in the interest of national security). Those reported figures are up 8 percent over the number of original classification decisions reported in FY 2002.

What I find most troubling, however, is that some individual agencies have no real idea how much information they generate is classified; whether the overall quantity is increasing or decreasing; what the explanations are for such changes; which elements within their organizations are most responsible for the changes; and most importantly of all whether the changes are appropriate (i.e., whether too much or too little information is being classified and whether for too long or too short a period of time). The identification of baseline information such as this would help agencies ascertain the effectiveness of their classification efforts.

My current concerns extend to the area of declassification as well. One of the principal procedures for maintaining the effectiveness of the classification system is the purging from the safeguarding system of information that no longer requires protection in the interest of national security. In addition to processes such as automatic and systematic declassification, as well as mandatory declassification reviews, the Executive Order clearly states that "information shall be declassified as soon as it no longer meets the standards for classification" (§ 3.1). Elsewhere, the Order specifically prohibits the use of classification "to prevent or delay the release of information that does not require protection in the interest of the national security" (§ 1.7 (a) (4)). Declassification cannot be regarded as a "fair weather project," something we tend to when resources are plentiful but which quickly falls off the priority list when times get tough, especially in times of national security challenges. Nonetheless, it is disappointing to note that declassification activity has been down for the past several years.

In some quarters, when it comes to classification in times of national security challenges, when available resources are distracted elsewhere, the approach toward classification can be to "err on the side of caution," by classifying and delaying declassification "when in doubt" and "asking questions later." Yet, the classification system is too important, and the consequences resulting from improper implementation too severe, to allow "error" to be a part of any implementation strategy. Error from either perspective, both too little and too much classification, is not an option. Too much classification unnecessarily impedes effective information sharing, and inappropriate classification undermines the integrity of the entire process. Too little classification can subject our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations to potential harm. It is in this regard that proactive oversight by an agency of its security classification program is crucial. To allow information that will not cause damage to national security to remain in the classification system, or to enter the system in the first instance, places all classified information at needless increased risk.

In response to these concerns, I have recently written to all agency heads asking them to closely examine their efforts in addressing the basics in establishing and maintaining an effective security classification program at their agency. All have been asked to give special emphasis to reviewing how they provide their personnel who deal with classified information the knowledge and understanding required to make the program work, and what positive steps they take to ensure the continued integrity of the system. This

includes ensuring that information that requires protection is properly identified and safeguarded; and, equally important, that information not eligible for inclusion in the classification system remains unclassified or is promptly declassified.

It is essential to recognize that the security classification system is permissive, not prescriptive – it identifies what information can be classified, not what information must be classified. The decision to classify information or not is ultimately the prerogative of an agency and its original classification authorities. The problem, however, is, with all due apologies to John Donne, no agency is an island. The exercise of agency prerogative to classify certain information has ripple effects throughout the entire executive branch. For example, it can serve as an impediment to sharing information with another agency, or with the public, who have a genuine need-to-know for the information. In addition, under some circumstances, it can actually undermine individuals' confidence in the integrity of the overall system, to include cleared individuals, an outcome with serious implications for everyone.

The 9/11 Commission has recommended that "Information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge". The Administration is currently developing guidelines and regulations to improve information-sharing both among Federal Departments and Agencies and between the Federal Government and state and local entities. On August 2, 2004, President Bush announced that he will be issuing a directive requiring all relevant

agencies to complete the task of adopting common databases and procedures so that intelligence and homeland security information can be shared and searched effectively, consistent with privacy and civil liberties.

I commend the President's leadership in this area, and my office, working through the appropriate agencies, will be examining and advising on issues relating to the "need-to-know" and the "third-agency rule," as set forth in E.O. 12958, as amended. The current framework governing the safeguarding of classified information is based upon the "push" model of information management. The need-to-know principle and the third-agency rule give the authorized holder of the information the sole prerogative of determining whether a prospective recipient requires access to specific information (see § 4.1 (c) of the Order). The Executive Order goes on to state that classified information originated in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency (§ 4.1 (i)). These principles reflect the premise that national security considerations always necessitate the restriction of the dissemination of classified information and that originators of classified information are omniscient and are cognizant of all possible uses of the information. As pointed out by the "9/11 Commission," the reality is that national security can be placed at risk if classified information is not effectively shared.

In the final analysis, it is the people who deal with the information, their knowledge and understanding of the program, their faith in the integrity of the system represented by the classification markings, and their belief that everyone in the executive branch will do

what is expected of them that protects truly sensitive information from unauthorized disclosure. This knowledge, understanding, confidence, and expectation cannot be taken for granted. The integrity of the system will not be maintained on its own. It requires clear, forceful and continuous effort by senior leadership to make it happen. And the integrity of the security classification program is essential to our nation's continued well-being. The consequences of failure are too high. Thus, the American people expect and deserve nothing less than that we get it right each and every day.

Again, I thank you for inviting me here today, Mr. Chairman, and I would be happy to answer any questions that you or the Subcommittee might have.

Mr. SHAYS. Ms. Haave.

Ms. HAAVE. Good morning, Chairman Shays, Mr. Kucinich, and members of the panel.

I appreciate the chance to speak with you today about the protection of classified information within the Department of Defense. My opening statement will be brief, as I believe the time we have here can best be spent in direct dialog.

Protection of classified information is one of the most important priorities of the Department. No one wants to provide information outside of proper channels that would do our servicemen and women, as well as our civilian coworkers harm. Nor does anyone want to give away what is our economic and military advantage by providing information about advanced science and technology, sources or methods of our operations.

The question becomes, how do we balance the risk of disclosure and its often incalculable consequences against the public's desire to know? The issue before us today is overclassification and whether it is an impediment to information sharing.

I have not found within the Department of Defense that people are intentionally overclassifying. That's not to say that it doesn't and isn't happening. More, I have found that these problems stem from time-driven, operational circumstances and a misunderstanding of classification guidance. In the end, people simply don't want to make mistakes that could have both personal and national security consequences.

Does this impact information sharing? Sometimes it does.

We in DOD are working to ensure our policies are clear about when and how to classify information, as well as ensuring personnel know and understand their responsibilities in sharing with those who must have the information.

Much data that is transported on DOD networks is protected by classification guidance provided by other government organizations. We adhere to that guidance, but we certainly can improve the way we do it. For example, how do we deal with originator-controlled documents in an electronic environment?

The 21st century is about information technology. It is about the seamless availability of information across security domains consistent with the governance strategy that ensures people are properly vetted and trained.

The collectors of information and also, normally, the original classifiers can never know the myriad ways that their information might be used for good purpose. Therefore, we have to migrate to a user-driven environment to support true competitive intelligence, to ensure the warfighters and policymakers have the information that they need to make good decisions, and to mutually support other organizations and agencies in successfully accomplishing their missions as well.

We must break down the functional stovepipes and institutional barriers in favor of a more horizontally integrated collaborative enterprise characterized by cooperation and incentivized, shared goals. We must make better use of all-source analysis to blur the origin of information and right to release using automated terror lines.

"Need to know," while still a valid concept that drives information security, must now also include the need to share information more broadly at multiple classification levels, as well as in the unclassified public domain.

Technology is not the problem. The technology we need is here today, or is being developed, and there are any number of initiatives that are moving us collectively in the right direction. Instead, I would offer that the problem is institutional and cultural, and no agency or organization is immune. Change is always difficult and fear of making a mistake precludes people from moving forward in ways that are consistent with technology and business process improvements.

In the end, this is a discussion about risk. How much risk is the Nation willing to endure in the quest to balance protection against the public's desire to know? It is a complex question that requires thought and, ultimately, action.

The Department of Defense has been taking that action with respect to information that it alone controls. As stated in my formal statement, the Department has embraced a network-centric enterprise with common standards and protocols and a robust information assurance and protection schema. But this architecture and enterprise are not cheap, and when extended to other governments, as well as State, local and other organizations, the costs are high.

We are working closely with the intelligence community, the Department of Homeland Security, and others to extend the enterprise, to facilitate the collaboration and cooperation that the public deserves, and we are better for it.

Thank you.

Mr. SHAYS. Thank you very much, Ms. Haave.

[The prepared statement of Ms. Haave follows:]

STATEMENT FOR THE RECORD

BY

MS CAROL A. HAAVE

DEPUTY UNDER SECRETARY OF DEFENSE
COUNTERINTELLIGENCE AND SECURITY

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS AND INTERNATIONAL RELATIONS

COMMITTEE ON GOVERNMENT REFORM

U. S. HOUSE OF REPRESENTATIVES

AUGUST 24, 2004

INTRODUCTION

Mr. Chairman, members of the Committee. Thank you for the opportunity to speak with you about the Department of Defense's classification management program and what we are doing to protect classified information while fostering an environment that allows extensive sharing without compromising critical sources and methods or operations. It is a delicate balance that we strive to achieve, one that is important for the Government and the public it represents.

BACKGROUND

National concern about protecting "secrets" was codified in 1917 when the Congress passed the first Espionage Act. At that time violations of the law could result in "punishment by a fine of not more than $10,000 or by imprisonment for not more than two years, or both" -- presumably a serious consequence in those days. Since then, we have continued to affirm the need for such laws to classify information deemed critical to the security of the United States, although they have remained relatively unchanged since 1940 when President Roosevelt signed Executive Order 8381 creating three levels of classification and specifying the "authorities" as to who could classify information. Over the subsequent decades, changes have been made that reflect the Government's, either more liberal or conservative philosophy about "secrets." Today, Executive Order (EO) 12958, "Classified National Security Information" as amended recently by EO 13292 governs how we classify, safeguard and declassify national security information.

THE DEPARTMENT OF DEFENSE PROGRAM

Within the Department of Defense, we implement classification and declassification policies through the DoD 5200.1-R, "Information Security Program Regulation," most recently updated in April 2004. That regulation is based upon the EOs cited above, as well as the Information Security Oversight Office (ISOO) Directive Number 1, "Classified National Security Information." In 1998 DoD and the Central Intelligence Agency (CIA) agreed to have uniform lexicon and methodology for showing classification markings. That methodology is captured in the Intelligence Community Classification and Control Markings Register.

There are two types of classifiers – original classification authorities (OCA) and derivative classifiers. OCAs are senior ranking officials within the Department who have been delegated the authority to classify information over which they have jurisdiction. For example, the Secretary of Defense, the Chairman of the Joint Chiefs of Staff and the Under Secretary of Defense for Policy have the authority to classify information up to Top Secret*. Those who use or restate information originally classified by one of the above are required to apply the original classification guidance. OCAs can assign one of three levels of classification to information – Confidential, Secret, or Top Secret. The level is determined by the seriousness of the damage that would be caused if the information were compromised. Additionally, there are program access designations and dissemination control markings** such as "Not Releasable to Foreign Nationals" (NOFORN) and "Dissemination and Extraction of Information Controlled by Originator" (ORCON) that further limit the extent to which information may be shared.

According to the EO, information pertaining to military plans, weapons, operations, intelligence activities, scientific and technological matters, vulnerabilities or capabilities of systems and foreign government information may be classified, if its disclosure would be injurious to the nation's security. The decision to classify, or not, certain information is a risk determination. OCAs develop classification guides (similar to handbooks) that indicate what information about a system, plan, program or project is classified and the appropriate markings that are to be used. Within the Department, we have an index of about 3000 classification guides. For example, there are classification guidelines for Operation Enduring Freedom and Iraqi Freedom, as well as most acquisition programs.

Since 9/11, and in times of war, it is not inconceivable that more information would be classified. However it should also be noted that the Department of Defense is also responsible for almost half of the information that has been declassified since 1995.

* Sensitive Compartmented Information (SCI) is the purview of the Director for Central Intelligence (DCI) in accordance with (IAW) DCI Directive (DCID) 6/1.
** Dissemination markings are also under the purview of the DCI IAW DCID 6/6.

One key concern in this discussion is that of unauthorized public disclosures of classified information. This unilateral, unapproved declassification compromises sources and methods, which damages intelligence and operational capabilities, may result in loss of life, breaches with cooperating governments and reveal dangerous vulnerabilities of US persons, US installations and this country. These lessen the Department's ability to protect critical information, technologies and programs—and they appear to be increasing at an alarming pace. Unauthorized disclosures demoralize those who are adhering to the standards of classification and their security agreements, has the potential to minimize the return on investment of taxpayer dollars when science and technology advantages are compromised, and may put the nation at risk. The Department continues to assess and improve its security education, training and awareness program to address this and other important security matters.

The DoD has an active classification management oversight program that is conducted de-centrally at multiple levels throughout the Department. Components are responsible for ensuring that OCAs are trained, conducting self-inspections to ensure compliance and providing information annually about the state of their classification management efforts to the Office of the Secretary of Defense (OSD) and ISOO. At the OSD level, oversight consists of providing classification management training coursework and conducting program, security and classification guidance reviews.

In the future, one could envision the process of classification and declassification to be easier. It will still require that people classify information appropriately. This is a training issue and the Department is creating an updated, web-based course accessible by all who need it. It will also require that we recognize the need for seamless availability and integration of multiple levels of classified and unclassified information among Federal, state, local and other organizations. Data from each of these entities are governed by their own unique statutory requirements.

The Department of Defense has embraced the 21st century information technology revolution. We are deploying the Global Information Grid, an enterprise architecture, to network all users in a common environment and with common services. We are mandating metadata and other standards to facilitate sharing across networks and among applications to foster collaboration and situational awareness. We are continuing to research and employ the latest technological advances, i.e., Internet protocol (IP)-based,

high speed, bandwidth on demand, and are investing heavily in persistent-continuous Information Assurance. We are developing cross-domain security solutions that will allow information to flow seamlessly between multiple classification levels. We have established a worldwide Public Key Infrastructure (PKI) for "trusted" network access control and user authentication for over three million DoD personnel as well as a PKI Federal Bridge to facilitate interoperability across the Federal Sector that includes contractors and vendors. The vision is a user-driven, "smart-pull," highly trusted and networked, seamless, cross security domain environment that allows cooperation and collaboration among those who have been properly vetted. And while there is much being done, there is much more to do.

The decision to classify or not is a risk decision and not one the Department takes lightly. We continuously strive to balance the public's desire for information with the protections necessary to ensure the safety and security of our nation that is more at risk today than ever before.

I thank you for the opportunity to address this critical challenge.

Mr. SHAYS. Mr. Aftergood.

Mr. AFTERGOOD. Thank you, Mr. Chairman.

I was going to begin by attempting to document for you the state of the classification system as it is perceived from outside the government. I was going to explain to you that classification policy is often arbitrary, inconsistent, that classifiers sometimes classify contrary to their own rules. Sometimes, as in the case of the Taguba report, they use classification to conceal criminal activity, and the classification system is, in other ways, unsatisfactory.

I have documented some of those rather serious charges in my formal testimony. I know from your opening statements that all of you already are aware of many of these problems.

Mr. SHAYS. Let me ask how long would it take for you to do that.

Mr. AFTERGOOD. I can do it very quickly.

Mr. SHAYS. I would like it to be part of the public record. So you have the time to do it. In the course of your presenting those documents, it gives us something to question everybody with.

Mr. AFTERGOOD. OK. I will do that briefly.

Mr. SHAYS. We will start the clock over again.

Mr. KUCINICH. Mr. Chairman, if I may, I think the witness ought to feel very comfortable in going over this material with the committee, and we eagerly await your recitation of your report.

Mr. AFTERGOOD. Thank you very much. I have selected not quite at random, but a cross-section of cases that have come into my hands that include several anomalies in classification policy.

The recent Senate intelligence report on prewar intelligence on Iraq included abundant redactions, that is, removals of information from the report that in some cases were inconsistent or inexplicable.

On one page attached to my testimony it was stated that Iraqi agents agreed to pay up to a "deleted" amount for certain aluminum tubes. This is a point of controversy having to do with Iraq's nuclear weapons program. But on another page of the same report, CIA reviewers included the very same information: Iraqi agents agreed to pay up to $17.50.

At a minimum, this is inconsistent. It shows a lack of professionalism in classification; but more than that, I think it shows an improper attempt to withhold information that has no business being classified. Obviously, the Iraqis know what they paid. The vendors know what they paid. They know that we know. There is nothing sensitive that's being concealed here, but it held up the release of the report, and it helped turn it into a kind of Swiss cheese.

A second example is the Taguba report on abuses of prisoners at Abu Ghraib prison in Iraq. As you can see from the title page of the report, which is also appended to my testimony, the whole report was classified as Secret. That is, the Secret classification level means that its disclosure could reasonably be expected to cause serious damage to national security.

If you look at page 16 of the report, you can see that several individual paragraphs of the report were also classified Secret, such things as a finding that numerous incidents of sadistic, blatant and wanton criminal abuses were inflicted on detainees; punching, slap-

ping and kicking detainees; jumping on their naked feet and so on. These individual findings were classified Secret.

That is not only inappropriate, it actually is a violation of the rules governing the classification system itself. Those rules state in President Bush's executive order that in no case shall information be classified in order to conceal violations of law. Yet it appears that is exactly what happened here. When agencies violate their own classification rules, one thing that tells you is that oversight is inadequate.

A third example that I pulled from my written statement is, to me, the most extreme example of overclassification, and that has to do with CIA's insistence on classifying historical intelligence budget data. In 1997 and 1998, the CIA declassified, under pressure of litigation, the total intelligence budget for those years, for 1997 and 1998. But in 2000 they said that similar information from 50 years earlier is still properly classified.

To state the obvious, that is a logically incoherent position. There is no national security construct that permits the declassification of the 1997 budget, but prohibits the declassification of the 1947 budget.

What that tells me is that the CIA has completely lost its bearings when it comes to classification of budget information, and that there is no one to stop them from arbitrary and mistaken classification actions.

There are many other examples. The document you entered into the record, Mr. Chairman, "Dubious Secrets," from the National Security Archive, is filled with other cases. I imagine that anyone who has had dealings with the national security system, either as a government employee or as a concerned citizen, has their own horror stories to tell. Certainly the public is increasingly becoming concerned.

I am a member of the steering committee of a new coalition of politically diverse organizations under the rubric openthegovernment.org, that has come together to try to remedy this situation.

I would just like to say one final word about what is in a way the most important aspect of this hearing. That is, what's the solution? The solution is not a broad policy critique. I don't think the solution is to try to fix the whole system at a single blow. I think the solution was identified by the 9/11 Commission. That is start with a very specific, tangible change. Start with declassification of intelligence budget information. There is no other category of information that has been as vigorously maintained as Secret for so long with so much energy as intelligence budget information. If we can fix that, then the road becomes clear to fixing a whole range of other erroneously or improperly classified categories of information; and that's the point I wanted to stress.

Thank you very much.

Mr. SHAYS. Thank you, Mr. Aftergood.

[The prepared statement of Mr. Aftergood follows:]

Prepared Statement
of
Steven Aftergood
Federation of American Scientists

before the
Subcommittee on National Security
House Committee on Government Reform

"Too Many Secrets:
Overclassification as a Barrier to Critical Information Sharing"

August 24, 2004

Mr. Chairman, thank you for the opportunity to testify today.

I am a senior research analyst at the Federation of American Scientists, a policy research and advocacy organization concerned with science and national security. I direct the FAS Project on Government Secrecy, which aims to reduce the scope of national security secrecy and to promote enhanced public access to government information. I write the email newsletter *Secrecy News*, which monitors developments in government information and intelligence policies. My project has not been the recipient of federal funding or contracts.

Introduction

The 9/11 Commission performed an important service by identifying overclassification as an impediment to information sharing and more generally as an obstacle to oversight and accountability.

Even under optimal circumstances, there will always remain a tension between the need to protect certain types of highly sensitive information and the need to share such information with those who can put it to good use in the service of national security. But present circumstances are far from optimal.

National security classification policy today is erratic, undisciplined and prone to abuse.

To illustrate the problem, I will cite three recent examples of dubious classification decisions, which are documented in the attachments to this testimony, and then outline some directions forward.

Some Recent Classification Errors and Abuses

I. The Classified Cost of Aluminum Tubes

The cost of aluminum tubes that were acquired by Iraq was deleted by CIA classification officials from one page of the recent Senate Intelligence Committee report on pre-war intelligence on Iraq.

But the very same information was disclosed on another page of the same report.

Thus, on page 96 of the report (attached below), it was noted that "Iraqi agents agreed to pay up to [deleted] for each 7075-T6 aluminum tube. Their willingness to pay such costs suggests the tubes are intended for a special project of national interest."

Then, on page 115 (also attached), the report stated: "Iraqi agents agreed to pay up to U.S. $17.50 each for the 7075-T6 aluminum tube. Their willingness to pay such costs suggests the tubes are intended for a special project of national interest."

Clearly a mistake was made here, either by deleting the cost information on the earlier page or by disclosing it on the later page.

I believe that it was an error of overclassification, and that the cost information should not have been deleted. Certainly the Iraqis know the amount that they agreed to pay for the aluminum tubes, as do the tube vendors. They also know that we know the amount, since that fact was not withheld by the CIA reviewers.

So no valid national security purpose was served by classifying the tube cost. Instead, CIA reviewers erected an arbitrary barrier to disclosure. The fact that they did so imperfectly and inconsistently is small consolation.

II. The Classification of Criminal Activity at Abu Ghraib Prison

By classifying a report on the torture of Iraqi prisoners as "Secret," the Pentagon may have violated official secrecy policies, which prohibit the use of classification to conceal illegal activities.

The report, authored by Maj. Gen. Antonio Taguba, found that "between October and December 2003, at the Abu Ghraib Confinement Facility, numerous incidents of sadistic, blatant, and wanton criminal abuses were inflicted on several detainees."

"The allegations of abuse were substantiated by detailed witness statements and the discovery of extremely graphic photographic evidence," Gen. Taguba wrote in paragraph 5, page 16 of his report (attached).

This specific observation, as well as the itemized list of criminal activities on paragraph 6 of the same page, and the report as a whole, were all classified "Secret / No Foreign Dissemination" (see title page, attached).

Such classification may have been more than simply inappropriate. It appears to have been a violation of official policy, which forbids the use of secrecy to cover up crimes.

That policy states in Section 1.7 of Executive Order 12958, as amended (EO 13292):

> "In no case shall information be classified in order to ... conceal violations of law, inefficiency, or administrative error [or to] prevent embarrassment to a person, organization, or agency...."

If it is true that the classification system's own rules were violated in this case, as I believe, then that is a sign that there is insufficient oversight to enforce existing rules.

III. The Classification of Historical Intelligence Budget Data

In what may be the most extravagant current case of overclassification, the Central Intelligence Agency contends that 50 year old intelligence budget figures are still properly classified today.

To fully appreciate the baselessness of the CIA position, it is important to realize that the Agency itself declassified the total intelligence budget (in response to Freedom of Information Act litigation) for Fiscal Year 1997 and 1998.

But thereafter, in December 2000, Agency officials said that similar information from half a century earlier could not be released. (See the 12/14/00 CIA letter, attached).

This is not simply a disagreement over a matter of policy – it is a sign of radical incompetence on the part of CIA classification officials. What is worse is that there is no effective check on such erratic behavior.[1]

Steps Towards a More Rational Classification Policy

There is no single prescription that will cure all of the defects in current classification policy. In fact, it may be that national security secrecy, even when indisputably necessary, will always be an anomaly and an irritant in a democracy.

[1] This matter is currently the subject of litigation under the Freedom of Information Act in DC District Court (*Aftergood v. CIA*, Case No. 01-2524).

Even so, there are important steps that can be taken both to limit overclassification and to enhance the integrity of the national security classification system. These include the following.

1. Declassification of Intelligence Budgets

The 9/11 Commission wisely identified intelligence budget disclosure as an important first step in reversing overclassification:

> To combat the secrecy and complexity we have described, the overall amounts of money being appropriated for national intelligence and to its component agencies should no longer be kept secret. (Commission report, page 416)

This is a modest but exceptionally astute recommendation. Several aspects of intelligence budget disclosure make it an outstanding starting point for classification reform.

First, it is a very specific, non-rhetorical secrecy reform. It will be clear to all whether or not it has been implemented.

Moreover, budget disclosure is a defining characteristic of our system of government. Budget data are one of only two categories of government information whose publication is specifically required by the U.S. Constitution (in Article I). (The other category is the Journal of the Congress).

Most important of all, the secrecy of intelligence appropriations is perhaps the preeminent symbol of the cold war secrecy system, and its rejection will signal the overcoming of that inherited system.

No other single category of secret government information has been as fiercely defended by proponents of official secrecy for so long as the size of the intelligence budget. Indeed, the very subject of budget secrecy has become a kind of totem or fetish such that half century-old figures are still officially withheld, as noted above.

If such a deeply entrenched symbol of reflexive secrecy can finally and permanently be overcome, it will clear a path to the rethinking of other poorly justified secrecy policies within the intelligence community and beyond.

2. Expanded Executive Branch Oversight of Classification Activity

One unheralded success story in the world of classification policy is the role of the Interagency Security Classification Appeals Panel (ISCAP), a body established by executive order 12958 to consider appeals from the public of document declassification requests that have been denied (among other duties).

Although it is composed of representatives of five executive branch agencies – the CIA, Department of Defense, Department of State, Department of Justice and NARA – the Panel has overruled the classification decisions of its own member agencies in about 70% of the appeals that it has considered since 1996.

This surprising record confirms that overclassification is a real problem but also points the way towards a solution: increased oversight and review of classification activity within the executive branch itself.

Such internal executive branch oversight could take various forms—an expansion of the valuable but miniscule Information Security Oversight Office; creation of agency ombudsmen whose task is to supervise classification activity with an eye toward eliminating excessive secrecy; regular periodic inspector general audits of classification practices within the key national security agencies; and so on.

Such oversight should not be viewed as a concession to critics or a mere gesture towards abstract values of "openness." To the contrary, whether they realize it or not, executive branch agencies have a material interest in reducing unnecessary secrecy, which imposes severe financial and operational costs on their performance.

3. Enhanced Congressional Oversight of Secrecy Policy

If the proper conduct of national security classification policy is important, which it plainly is, then it is also an important subject for congressional oversight. But routine, systemic oversight of classification policy has often been lacking.

In 1997, a Congressionally-mandated Commission on Protecting and Reducing Government Secrecy (the "Moynihan Commission") produced an outstanding report on the problems of secrecy and proposed a series of recommended reforms, including legislative actions. For the most part, the Commission recommendations were ignored.

On the other hand, this Committee's important hearings on Presidential records and other information policy issues in recent years suggest that even more attention could be usefully turned to the subject.

Such oversight need not be an arduous or elaborate undertaking. It can be as simple as posing a question to the Pentagon: Why was the Taguba report on the abuse of Iraqi prisoners classified as a national security secret? Or to the CIA: Why are 50 year old budget data still withheld from public disclosure?

The Information Security Oversight Office already reports to the President annually on the state of classification and declassification activity throughout the executive branch. It may be that the submission of this report would serve as a convenient occasion for regular annual hearings on the subject.

Congress should also give careful consideration to the pending proposal for an Independent National Security Classification Board, as set forth in H.R. 4855.

4. Invigorated Judicial Review

In the Freedom of Information Act, Congress mandated *de novo* judicial review of agency decisions to withhold information, including classified information, from public disclosure.

But over the years, the strong review that Congress established has diminished nearly to the vanishing point in favor of a doctrine of "judicial deference," i.e. deference to the executive branch on questions of national security secrecy.

According to this view, courts are wholly unqualified to assess the substantive legitimacy of classification decisions (though they may rule on procedural adequacy) and they must accept the assurances of agency officials that contested information is properly classified.

In effect, through a series of unfortunate precedents, the courts have abdicated the judicial function when it comes to the review of agency classification decisions.

This explains the astonishing disparity between the executive branch ISCAP -- which, as noted above, has overturned classification decisions in the majority of cases it has considered in recent years -- and the judicial branch, which has overturned essentially zero classification decisions.

By now, the effectiveness of the Freedom of Information Act as a mechanism for classification oversight has been severely curtailed.

Therefore: Congress could restore the vitality of the Act with an amendment to strengthen judicial review of contested classification decisions. Such review might permit judicial deference to the executive branch -- but would no longer require it as a matter of course.

5. Limit the Definition of Intelligence "Sources and Methods"

Perhaps the single most penetrating measure that Congress could enact to combat excessive secrecy in U.S. intelligence would be to amend the requirement to protect intelligence sources and methods, so as to limit such protection to those cases it is justified by national security concerns.

Pursuant to 50 U.S.C. 403-3(c)(7), the Director of Central Intelligence is obliged to "protect intelligence sources and methods from unauthorized disclosure."

Maximizing its secrecy authority, the CIA interprets this statute liberally to include any and all intelligence "sources and methods," even those that do not warrant national security classification.

As a result, even the most mundane information is buried under a blanket of secrecy. How many subscriptions to the New York Times does the CIA have? How much does the Agency spend on stationery or pens and pencils? All such information is guarded as if the very future of liberty depended upon it.

Much of this arbitrary secrecy could be eliminated at a single stroke if Congress specified that the DCI is obligated to protect only those intelligence sources and methods that could be jeopardized or compromised by disclosure.

Some Other Issues

In the interest of brevity, I would like to mention two other issues of significance, without fully exploring them at this time.

1. The Proliferation of Controls on Unclassified Information

The 9/11 Commission focused on the problem of overclassification as an impediment to information sharing. But a comparable and possibly greater problem is due to expanding controls on unclassified information.

A plethora of new controls is increasingly being applied to unclassified information, including information that was formerly in the public domain.

These controls are denominated by various terms: Sensitive But Unclassified (SBU), Sensitive Security Information (SSI), Sensitive Homeland Security Information (SHSI), Law Enforcement Sensitive (LES), Critical Infrastructure Information (CII), Critical Energy Infrastructure Information (CEII), For Official Use Only (FOUO), Unclassified Controlled Nuclear Information (UCNI), Limited Official Use (LOU), and so forth and so on.

These are multiple, overlapping and sometimes inconsistent control systems that replicate features of the national security classification system such as "need to know" in an irregular, haphazard way. Thus, for example, the Department of Homeland Security now requires a non-disclosure agreement to be executed for access to "sensitive but unclassified" (SBU) information.

Whereas the classification system has at least some internal and external constraints and prohibitions, the new controls on unclassified information are largely unchecked.

This is a recipe for chaos that has not yet received the attention it deserves.

2. The "Dark Side" of Information Sharing

It is often taken for granted that information sharing among government agencies and with state and local officials is an unalloyed good. Indeed, the failure to share information is one of the clearest problems identified by the investigations into September 11.

But efforts to lower barriers to access for government officials in order to enhance information sharing often entail raised barriers to access for members of the general public.

Vast amounts of formerly public information has been removed from the public domain. The non-disclosure agreements that state and local officials sign as a condition of information sharing threaten to become walls between those officials and the communities that they serve.

It seems that a decision has been tacitly made that the American public does not have a "need to know" any information that some unaccountable official has determined is suitable "for official use only." This is unsatisfactory.

While some new controls on unclassified information are bound to be justified, they need to be matched by new mechanisms for reviewing and challenging decisions to withhold such information from the public. Up to now, such mechanisms have been lacking.

Conclusion

The complexity of government information policy is matched and exceeded by its importance. More than any organizational or structural reform, improvements in information policy will pay immediate dividends in performance.

But merely talking about improvements and criticizing overclassification is not enough. Action is now required.

The first order of business, as the 9/11 Commission recommended, should be the disclosure of intelligence budget appropriations. That will set the stage for a continuing process of classification reform and revision that is long overdue.

Thank you again for convening a hearing on this important subject.

[redacted]

REPORT ON THE U.S. INTELLIGENCE COMMUNITY'S PREWAR INTELLIGENCE ASSESSMENTS ON IRAQ

Ordered Reported on July 7, 2004

SELECT COMMITTEE ON INTELLIGENCE

UNITED STATES SENATE

108th CONGRESS

PAT ROBERTS, Kansas, *Chairman*
JOHN D. ROCKEFELLER IV, West Virginia, *Vice Chairman*

ORRIN G. HATCH, Utah
MIKE DEWINE, Ohio
CHRISTOPHER S. BOND, Missouri
TRENT LOTT, Mississippi
OLYMPIA J. SNOWE, Maine
CHUCK HAGEL, Nebraska
SAXBY CHAMBLISS, Georgia
JOHN W. WARNER, Virginia

CARL LEVIN, Michigan
DIANNE FEINSTEIN, California
RON WYDEN, Oregon
RICHARD J. DURBIN, Illinois
EVAN BAYH, Indiana
JOHN EDWARDS, North Carolina
BARBARA MIKULSKI, Maryland

BILL FRIST, Tennessee, *Ex Officio*
THOMAS A. DASCHLE, South Dakota, *Ex Officio*

[redacted]

[redacted]

(3) Iraqi agents agreed to pay up to [redacted] for each 7075-T6 aluminum tube. Their willingness to pay such costs suggests the tubes are intended for a special project of national interest.

(4) Iraq has insisted that the tubes be shipped through such intermediary countries as [redacted] in an attempt to conceal the ultimate end user; such activity is consistent with Iraq's prewar nuclear procurement strategy but are more robust than post-war denial and deception (D&D) efforts.

(5) Procurement agents have shown unusual persistence in seeking numerous foreign sources for the tubes, often breaking with Iraq's traditionally cautious approach to potential vendors.

(6) An aluminum tube built to the Iraqi specifications for the tubes seized [redacted] was successfully spun in a laboratory setting to 60,000 rpm (1000Hz). This test was performed without balancing the tube; a critical step required for full speed operation, but still provided a rough indication that the tube is suitable as a centrifuge rotor.[15]

(7) The dimensions of the tubes [redacted] are similar to those used in the Zippe and Beams-type gas centrifuges. The inner diameter of the seized tubes - 74.4 mm – nearly matches the tube size used by Zippe and is described in detail in his unclassified report on centrifuge development. The length and wall thickness of the seized tubes are similar to Iraq's prewar Beams design.

(8) Iraq performed internal pressure tests to induce a hoop-stress level similar to that obtained by an operating rotor.

(9) [redacted]

(U) The NIE included discussion of some of these assessments in the main text and contained an annex with a more extensive discussion of the assessments and extensive dissenting opinions from both the DOE and INR. The following section outlines the intelligence and assessments provided by the intelligence agencies on the aluminum tubes.

---

[15] [redacted]

[redacted]

[redacted]

that in manufacturing rockets either a layer of insulating material is painted to the interior wall and the case is then filled with solid propellent, or a precast grain of solid propellant is loaded inside the tube cavity using thin metal spacers to separate the grain from the tube wall. In either case, minor surface imperfections would have no effect on the performance of the rocket. According to the IAEA, the finish of the Iraqi tubes that were intercepted [redacted] was worse than the finish on the older tubes Iraq declared in 1996. In addition, any machining Iraq had to perform to change the wall thickness of the tubes would also change the interior surface of the tubes, making a request for a smooth finish unnecessary if the tubes were intended to be used in a thin walled centrifuge.

([redacted]) (3) Iraqi Agents Agreed to Pay up to U.S. $17.50 Each for the 7075-T6 Aluminum Tube. Their Willingness to Pay Such Costs Suggests the Tubes Are Intended for a Special Project of National Interest

([redacted]) A [redacted] intelligence report does indicate, as the NIE notes, that Iraq may have agreed to a price of about U.S. $17.50 per tube in an attempt to procure aluminum tubes. Most reports showed, however, that Iraq had negotiated lower prices for the tubes, typically U.S. $15 to U.S. $16 per tube, and as low as U.S. $10 per tube [redacted]. The DOE told Committee staff that according to the IAEA [redacted] Iraq paid between [redacted] for each aluminum tube acquired in the 1980s. If inflation is taken into account, Iraq would be paying less today than in the 1980s for the same tubes. A DOE analyst also contacted a U.S. aluminum tube manufacturer to request a price quote for 7075-T6 aluminum tubes with similar dimensions to the Iraqi tubes. The analyst did not request specific tolerances which could have raised the price of the tubes. The U.S. manufacturer quoted a price of $19.27 per tube, higher than the price Iraq was able to negotiate.

(U) Furthermore, the NIE assessment about the cost of the tubes referenced the fact that Iraq was using 7075-T6 aluminum, which the NIE noted "is considerably more expensive than other, more readily available material." As noted previously, DOD rocket engineers told Committee staff that 7075-T6 aluminum is not more expensive that other suitable materials, suggesting that the use of 7075-T6 aluminum did not increase the cost of the tubes.

[redacted]

ARTICLE 15-6 INVESTIGATION OF THE 800th MILITARY POLICE BRIGADE

SECRET/NO FOREIGN DISSEMINATION

February 2004, COL Thomas M. Pappas was the Commander of the 205th MI Brigade and the Commander of FOB Abu Ghraib (BCCF). **(ANNEX 31)**

3. (U) That the 320th Military Police Battalion of the 800th MP Brigade is responsible for the Guard Force at Camp Ganci, Camp Vigilant, & Cellblock 1 of FOB Abu Ghraib (BCCF). That from February 2003 to until he was suspended from his duties on 17 January 2004, LTC Jerry Phillabaum served as the Battalion Commander of the 320th MP Battalion. That from December 2002 until he was suspended from his duties, on 17 January 2004, CPT Donald Reese served as the Company Commander of the 372nd MP Company, which was in charge of guarding detainees at FOB Abu Ghraib. I further find that both the 320th MP Battalion and the 372nd MP Company were located within the confines of FOB Abu Ghraib. **(ANNEXES 32 and 45)**

4. (U) That from July of 2003 to the present, BG Janis L. Karpinski was the Commander of the 800th MP Brigade. **(ANNEX 45)**

5. (S) That between October and December 2003, at the Abu Ghraib Confinement Facility (BCCF), numerous incidents of sadistic, blatant, and wanton criminal abuses were inflicted on several detainees. This systemic and illegal abuse of detainees was intentionally perpetrated by several members of the military police guard force (372nd Military Police Company, 320th Military Police Battalion, 800th MP Brigade), in Tier (section) 1-A of the Abu Ghraib Prison (BCCF). The allegations of abuse were substantiated by detailed witness statements **(ANNEX 26)** and the discovery of extremely graphic photographic evidence. Due to the extremely sensitive nature of these photographs and videos, the ongoing CID investigation, and the potential for the criminal prosecution of several suspects, the photographic evidence is not included in the body of my investigation. The pictures and videos are available from the Criminal Investigative Command and the CTJF-7 prosecution team. In addition to the aforementioned crimes, there were also abuses committed by members of the 325th MI Battalion, 205th MI Brigade, and Joint Interrogation and Debriefing Center (JIDC). Specifically, on 24 November 2003, SPC Luciana Spencer, 205th MI Brigade, sought to degrade a detainee by having him strip and returned to cell naked. **(ANNEXES 26 and 53)**

6. (S) I find that the intentional abuse of detainees by military police personnel included the following acts:

   a. (S) Punching, slapping, and kicking detainees; jumping on their naked feet;
   b. (S) Videotaping and photographing naked male and female detainees;
   c. (S) Forcibly arranging detainees in various sexually explicit positions for photographing;
   d. (S) Forcing detainees to remove their clothing and keeping them naked for several days at a time;
   e. (S) Forcing naked male detainees to wear women's underwear;
   f. (S) Forcing groups of male detainees to masturbate themselves while being photographed and videotaped;

Central Intelligence Agency

Washington, D.C. 20505

DEC 14 2000

Mr. Steven Aftergood
Senior Research Analyst
Federation of American Scientists
307 Massachusetts Avenue, N.E.
Washington, D.C. 20002

Reference: F95-0825

Dear Mr. Aftergood:

This is in response to your 5 June 1995 in which you appealed the 30 May 1995 determination of this agency in response to your 11 May 1995 Freedom of Information Act request for **"a copy of historical U.S. intelligence budget data from 1947 through 1970."**

Specifically, you appealed our determination to deny you access to information in its entirety on the basis of Freedom of Information Act exemptions (b)(1) and (b)(3).

Your appeal has been presented to the appropriate member of the Agency Release Panel, the Information Review Officer for the Director of Central Intelligence area. Pursuant to the authority delegated under paragraph 1900.43 of Chapter XIX, Title 32 of the Code of Federal Regulations (C.F.R.), the Information Review Officer has reviewed the material, the determinations made with respect to it, and the propriety of the application of the Freedom of Information Act exemptions asserted with respect to the material. It has been determined that the material must continue to be withheld in its entirety on the basis of Freedom of Information Act exemptions (b)(1) and (b)(3). Further, in regard to your appeal and in accordance with CIA regulations appearing at 32 C.F.R. paragraph 1900.41(c)(2), the Agency Release Panel has affirmed this determination.

Mr. Steven Aftergood

Exemption (b)(1) pertains to matters which are specifically authorized under criteria established by Executive Order 12958 to be kept secret in the interest of national defense or foreign policy and which are currently and properly classified.

Exemption (b)(3) pertains to information exempt from disclosure by statute. The relevant statutes are Subsection 103(c)(6) of the National Security Act of 1947, as amended, 50 U.S.C. § 403-3(c)(6), which makes the Director of Central Intelligence responsible for protecting intelligence sources and methods from unauthorized disclosure, and Section 6 of the Central Intelligence Agency Act of 1949, as amended, 50 U.S.C. §403g, which exempts from the disclosure requirement information pertaining to the organization, functions, names, official titles, salaries, or numbers of personnel employed by the Agency.

In accordance with the provisions of the Freedom of Information Act, you have the right to seek judicial review of this determination in a United States district court.

We appreciate your patience while your appeal was being considered.

Sincerely,

Gregory L. Moulton
Executive Secretary
Agency Release Panel

Mr. SHAYS. Mr. Crowell. I want to say it correctly. Is it Crowell?

Mr. CROWELL. It's Crowell. That's to avoid getting confused with a certain admiral that I'm always confused with.

Good morning, Chairman Shays, Mr. Kucinich, and members of the subcommittee. I would like to thank you for this opportunity to testify this morning on recommendations that are made by the Markle Foundation Task Force on National Security in the Information Age.

I think you will find that our observations are in agreement, Mr. Chairman, with your opening statement of the problem. The Markle Foundation Task Force is seeking, though, to outline and propose a new strategy of information sharing that can benefit our war on terrorism.

Information and information sharing are key to fighting terrorism and enhancing our security. Today, our government still does not have all of the information it needs to fight terrorism, and the information it does have is sometimes isolated in different agencies, and therefore it is more difficult to see its significance.

While the discussion about how to implement the 9/11 Commission's recommendation to restructure the intelligence community is important, another key 9/11 Commission recommendation that is creating and implementing a trusted information network to facilitate better information sharing among our intelligence and law enforcement organizations at the Federal, State and local levels could actually make America safer today.

The 9/11 Commission embraced the recommendations for creation of a System-wide Homeland Analysis and Resource Exchange, the acronym SHARE, network, made last December by the Markle Foundation Task Force on National Security in the Information Age.

The Markle Foundation Task Force consists of leading national security experts from four administrations, as well as widely recognized experts on technology and on civil liberties. The SHARE network concept represents a virtual reorganization of government by fundamentally altering how people in the many organizations ask to fight terrorism, how they share information to facilitate better and faster decisionmaking.

Such an approach when paired with strong divide lines that govern the system is also the best way to protect privacy and civil liberties. The SHARE network is aimed at moving us from our current need-to-know system into the need-to-share culture that you've been describing. However, one of the barriers to enabling that move involves classification and information-security practices.

Decisions about sharing intelligence in the Government today are still made largely in the context of a system of classification that was developed during the cold war. During the cold war, the use of information was dominated by a culture of classification and tight limitations on access in which information was shared only on the need-to-know basis.

The current system assumes that it is possible to determine in advance who needs to know particular information and that the risks associated with disclosure are greater than the potential benefits of wider information sharing. The results of the incentives currently in place to protect information results and far more infor-

mation being classified initially and remaining classified than is necessary or appropriate.

Another problem with the current system is that each agency has its own classification practices which leads to cultural tensions when agencies attempt to share information with each other. This cold war mindset of classification, sanitization and tight limits on sharing information is ill-suited to today's homeland security challenge. While certain information, particularly about sources and methods, must be protected against unauthorized disclosure, the general mindset should be one that strives for broad sharing of information with all of the relevant players in the network.

The Markle Foundation Task Force approach is to develop new concepts of operation and to use new technology to achieve a sharing culture. The SHARE network concept is a decentralized, loosely coupled, secure and trusted network that sends information to and pulls information from all participants in the system. Such an approach empowers all participants, from local law enforcement officers to senior policymakers.

Our approach combines policy and technical solutions to create a network that would substantially improve our ability to predict and prevent terrorist attacks. The SHARE network is based upon the right to share concept. By taking steps, by creating tear-line reports, it moves us from a system of classification to one that is based on authorization and encourages reports that contain the maximum possible amount of shareable information.

In addition, SHARE would use existing technologies that can facilitate the sharing of sensitive information with inappropriate channels and with protections for privacy. Screening tools can be used to help the redaction process to create less classified reports and can also tell us when sensitive information is about to be sent to parties who lack the proper permission to receive it.

To address the need for information about reliability of a source without having to rely on classified descriptions, we recommend the use of reputation meters, similar to those that are used today to rate sellers in e-bay in formats, and also to use standard formats for intelligence documents.

Auditing technology could be deployed to track the flow of information to different players and to record how the information is used, which could help deter leaks. Information-rights management technologies when combined with digital certificates can also help by allowing agencies to create self-enforcing rules about who can have access to particular documents, how they can be used and how long the documents can be viewed before access expires.

Finally, information can be accompanied by clear, more specific handling requirements and dissemination limitations.

In conclusion, Mr. Chairman, information sharing itself is not the goal. Rather, it is the means by which we can effectively enhance security and protect privacy, by maximizing our ability to make sense of all of the available information. To accomplish this, particularly in fighting terrorism, we must shed our current cold war need-to-know mentality and replace it with a culture based on need-to-share. Information security is a legitimate concern, but it can be appropriately addressed in the ways that I've outlined

above. What is needed now is the leadership by both Congress and the President to get the information flowing.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Crowell follows:]

Subcommittee on National Security, Emerging Threats, and International Relations
House Committee on Government Reform
August 24, 2004

Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing

Testimony of Bill Crowell
Markle Taskforce on National Security in the Information Age

Good morning Chairman Shays and members of the Subcommittee. I would like to thank you for the opportunity to testify this morning on the recommendations made by the Markle Foundation Task Force on National Security in the Information Age.

Information, and information sharing, are key to fighting terrorism and enhancing our security. Today, our government still does not have all of the information it needs to fight terrorism. And the information it does have is sometimes isolated in different agencies and therefore it is more difficult to see its significance. While the discussion about how to implement the 9/11 Commission's recommendation to restructure the intelligence community is important, another key 9/11 Commission recommendation, creating and implementing a "trusted information network" to facilitate better information sharing among our intelligence and law enforcement organizations at the Federal, State and Local levels could make America safer today.

Towards that end the 9/11 Commission embraced the recommendations for creation of a Systemwide Homeland Analysis and Resource Exchange (SHARE) Network made last December by the Markle Foundation Task Force on National Security in the Information Age. The Markle Foundation Task Force consists of leading national security experts from four administrations, as well as widely recognized experts on technology and civil liberties.

The SHARE Network represents a "virtual reorganization" of government by fundamentally altering how people in the many organizations tasked with fighting terrorism share information to facilitate better, faster decision-making. Such an approach, when paired with strong guidelines that govern the system, is also the best way to protect privacy and civil liberties.

The SHARE Network is aimed at moving us from our current need-to-know system into a need-to-share culture.

However, one of the barriers to enabling that move involves classification and information security.

Decisions about sharing intelligence in the government today are still made largely in the context of a system of classification that was developed during the Cold War. During the Cold War, the use of information was dominated by a culture of classification and tight limitations on access, in which information was shared only on a "need to know" basis.

The current system assumes that it is possible to determine in advance who needs to know particular information, and that the risks associated with disclosure are greater than the potential benefits of wider information sharing.

The result of the incentives in place to protect information results in far more information being classified initially—and remaining classified—than is necessary or appropriate.

Another problem with the current system is that each agency has its own classification practices, which leads to cultural tensions when agencies attempt to share information with each other. Government agencies currently rely on processes for "sanitizing" classified information so that it can be shared with other agencies. Some federal agencies sanitize some reports to remove source and method information. But the sanitized version is often still classified, and is usually designed for dissemination only to other federal agencies. Sanitization does not generally occur as a matter of course for many agencies, and no agency, to our knowledge, regularly produces a sanitized version of information that is unclassified and appropriate for wide-scale dissemination to state, local, and private sector entities. The sanitization process is also often slow and cumbersome.

This Cold War mind-set of classification, sanitizing and tight limits on sharing information is ill suited to today's homeland security challenge. While certain information must be protected against unauthorized disclosure, the general mind-set should be one that strives for broad sharing of information with all of the relevant players in the network. The system should be designed to address the enormous difficulty of discovering terrorist plans before they are executed and the needs of the analysts that must uncover these plans, balance against the security concerns on the sources and methods of the collectors. Or, as the 9/11 Commission noted in their report, "Information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge."

The Markle Task Force Approach: New Concepts of Operations and New Technology

The SHARE Network is a decentralized, loosely coupled, secure and trusted network that sends information to and pulls information from all participants in the system. Such an approach empowers all participants, from local law enforcement officers to senior policy makers. Our approach combines policy and technical solutions to create a network that would substantially improve our ability to predict and prevent terrorist attacks.

WRITE TO SHARE

The SHARE Network is based on the "write to share" concept and moves us from a system based on classification to one based on authorization. By taking steps like creating "tear line" reports, in which an agency produces a less classified, or unclassified version, along with the classified version, SHARE encourages reports that contain the maximum possible amount of sharable information.

In our suggested approach, the production of such alternate versions would be commonplace and automatic. And it would be a top priority. For example, an agency would create a "Top Secret/Code Word" report that reveals the source of the information; a "Secret" version that would not reveal the source, but might give explicit detail on the threat; and a "Sensitive But Unclassified" version that might only contain the necessary action the recipient agencies should take given their specific roles in the network (for example, to be on the lookout for certain individuals or indicators of specific terrorist activity).

INFORMATION SECURITY and AUDIT TECHNOLOGIES

In addition, SHARE would use existing technologies that can facilitate the sharing of sensitive information. For example, screening tools could be used to assist in the redaction process when moving information across security levels. Screening tools can automatically alert disseminators when potentially sensitive information is about to be transmitted, or when information may be about to be sent to parties that lack the requisite permission to receive it. Semi-automated systems could also suggest special-handling guidelines as well as who should be included on dissemination lists.

To address the need for information about reliability of a source without having to rely on classified descriptions, we recommend the use of "reputation meters" – similar to those used by e-bay to rate sellers –in formats for intelligence documents.

In addition, auditing technology, for example, could be deployed to track the flow of information to different players and to record how the information is used (whether, for example, it is printed, forwarded, or edited). This could help deter leaks. The auditing tools should use strong means of authentication that have forensic value (that is, they should be permissible in court to prove access). Information rights management technologies, when combined with digital certificates, can also help by allowing agencies to create self-enforcing rules about who can have access to particular documents, how they can be used, and how long the document can be viewed before access expires. Another possibility would be to make federal funding for information-sharing purposes contingent on the adherence to certain rules prohibiting unauthorized disclosure. Finally, information could be accompanied by clearer, more specific handling requirements and dissemination limitations. While none of these measures is perfect, a combination of such efforts might reduce the chance of unauthorized disclosure or uncoordinated action, and thereby foster a healthy environment for the sort of broad communication that we envision.

Conclusion

Recently, a number of agencies have been experimenting with creating systems to share information. For example the FBI is developing a new information-sharing policy and concept of operations that could instigate a "need-to-share" culture of distribution despite major barriers to adopt and implement the anticipated structure. And while this is a step

in the right direction, an agency-by-agency approach will not work. What is needed is a national framework that would enable change across the government as a whole and with state and local authorities as well to overcome the cultural barriers to information sharing.

Information sharing itself is not the goal; rather it is the means by which we can effectively enhance security and protect privacy, by maximizing our ability to make sense of all available information. To accomplish this, we must shed our current Cold War "need to know" mentality and replace it with a culture based on the "need to share." Information security is a legitimate concern but can be appropriately addressed in ways that I have outlined above. What is needed now is the leadership – by both Congress and the President – to get the information flowing.

Thank you.

Mr. SHAYS. Thank you, Mr. Crowell.

Let me just make a few observations before Mr. Ruppersberger begins the questions, and one is that I carry a basic view that when the executive branch gets more power, it must be accompanied with more legislative oversight. I also take the view that classification practices impede oversight by Congress for the public.

I have read, in my 17 years in Congress, confidential—in terms of the rates of classification, confidential documents, secret documents, top secret documents, and then we have compartmentalized with code-word access and special access and so on, but much what I've read under confidential and secret and, in some cases, top secret, but not obviously as often, it has been information I have wondered why it has been classified.

In a meeting I had with the chairman of the 9/11 Commission, Governor Kean said to me his biggest surprise was reading hours of information, wondering why in the world was this classified.

Just another observation, that yesterday we were talking about fighting a network called Al Qaeda. We were told we need a human and a communication network. This was in public diplomacy, and I'm hearing today, no, we need to break out of our stovepipes and have a data network. It's just interesting that the word network keeps showing up.

Finally, to conclude my observation, we have nearly 4,000 people classifying information, 14 million documents, but some of those documents could, literally, have been a book. They could be extensive. So even when I think of 14 million, the document could be small, you know, just bit of information, or it could just be pages and pages and pages of information.

So, in the end, I'm interested in is learning what the solution is. That's my interest, and we'll start with Mr. Ruppersberger.

You have 10 minutes. If you need to run over, we can be informal with this.

Mr. RUPPERSBERGER. Thank you, Mr. Chairman.

First, Mr. Leonard, in your opening statement, you said that each agency has its own classification criteria, but no agency is an island. This creates both confusion and inconsistency that impedes the necessary bounds for national security and transparency in a democracy.

My question is this, do you believe a National Security Intelligence Director would help to solve part of this problem if that person had the authority both—also budgetary control to implement the policies that are necessary, some of the recommendations in the 9/11 Commission Report, but especially as it deals with the issue we're talking about here today, overclassification, making sure that what is classified needs to be classified and what is not is not?

Mr. LEONARD. Thank you, Congressman.

One thing I don't want to do is to presuppose any particular outcomes, but let me address it along these lines.

Mr. RUPPERSBERGER. I'm asking your opinion. I know this is in debate now. The President has recommended a National Security Director. The issue of budgetary still is not there. We're trying to get information.

Let me say this. The reason I'm asking these questions and we're all here is, we have an opportunity, I think now, to really do some-

thing very positive as it relates to our national security and intelligence, and it's very important that, based on your expertise, we get your opinion.

Mr. LEONARD. Yes, sir.

Mr. RUPPERSBERGER. I know you are not speaking for the administration, but I'm asking, from your expertise, what your opinion would be as far as a National Security Director, as far as the budgetary issues are concerned, so that person might be able to implement what we're talking about here today.

Mr. LEONARD. Yes, sir. Let me address that along these lines.

One of the most significant challenges we have, I think, in this area is that we do have a basic framework for classification, as I mentioned, but superimposed upon that are multiple variations of the system which are all designed to achieve the same end. So, for example, currently, the DCI has his own unique authorities with respect to protecting sources and methods. The Secretary of Energy has his own unique authorities with respect to protecting atomic energy information. The director of NSA has his own unique authorities with respect to protecting communication security information. The Secretary of Defense has his own unique authorities with respect to protecting NATO-related information, and the list goes on and on and on and on.

Those variations are, I think, significant impediments to information sharing. When it comes to protecting information, I see it as a binary state: Either it's protected or it isn't protected. And we have all these variations on the system that have minor nuances and differences in terms of how we protect information, how we credit systems, how we mark them and things along those lines.

If a single individual had the authority, had the authority to overcome the existing statutory and regulatory authority that allows multiple agencies to come up with their own nuances and variations on the system, yes, I think that would be a good thing.

Mr. RUPPERSBERGER. In your opinion, do you feel that person would need budgetary control, also, of those agencies?

Mr. LEONARD. Let's put it this way, Congressman, it's one thing to have the authority to write regulations. There always has to be consequences for noncompliance with regulations. I find budgetary authority is one of the best means in which to get people's attention with respect to compliance and noncompliance of the regulations.

Mr. RUPPERSBERGER. I guess you need the power to do what you need to do, I guess.

Mr. LEONARD. Yes, sir.

Mr. RUPPERSBERGER. Mr. Aftergood, there was an intelligence open hearing, I believe last week or the week before, where they talked about the intelligence budget, and you addressed that in your testimony as far as whether or not that needs to be public. And I think there's a bipartisan consensus that there is a lot in the intelligence budget that could be made public, but there also was a concern that some of that should not be made public, and I think in your report you seem as if the whole budget.

I would be concerned that, line by line, could be very dangerous to both our military and to some of our CIA people or NSA people throughout the world. Could you give me your opinion on whether

or not you think that the whole budget should be out front and open or whether or not we should focus on the areas which could cause some type of problem to our people who are fighting and working for our national security?

Mr. AFTERGOOD. Yes, sir. I do believe that there are portions of the intelligence budget that should remain classified. I would be guided by the recommendations of the 9/11 Commission which said that the total, the top line number, as well as the individual agency budget totals should be made public but nothing beyond that. I think that's a reasonable middle ground that would provide oversight. It would break the logjam of secrecy in this area, but it would keep sensitive programs protected.

Mr. RUPPERSBERGER. OK. I'm going to ask—I don't know how long I have. It's a broad question to the whole panel, but the 9/11 Commission endorsed the creation of a decentralized, technologically advanced, trusted information network to make threat information more widely accessible and to reverse cold war paradigms and cultural biases against information sharing. The Commission noted such a network had been described in a task force report commissioned by the Markle Foundation, Mr. Crowell, but the concept has not yet been converted into action.

My question to the whole panel if we have time—and I know it's a broad question, but I would like your point of view—what would you recommend to Congress as to how you would start to implement the changes that need to be done in order to effectuate the issue that we're talking about here today, overclassification, need-to-know? I mean, there are many issues that need to be classified in that question. But we have a tremendous amount of volume. We have a lot of agencies.

Part of the problem in intelligence is just getting this enormous amount of volume on Internet and all that we get and then analyzing it and then getting it to the right people so they can implement and use it to protect our national security.

You have to remember now, we're focused on this. The country is focused. How would you begin to implement the changes that need to be made? You want to start with Mr. Crowell and then go down that way. Thanks.

Mr. CROWELL. Thank you very much. Let me start by saying that we have just concluded a preliminary session at the Aspen Institute in Colorado in which we were addressing the very issue that you raised, which is, what are the next steps for implementing a SHARE concept network? It's a very difficult problem, and it's a long kind of effort because it's a very large undertaking.

We believe that it begins with legislation that would essentially outline the kind of network that the Congress would like to see, based upon some of the principles which I will very briefly describe, and that the President then put together the cross-agency kind of implementing process that is necessary, because once you begin working across agencies, funding and management of large undertakings like this become very, very difficult and very complex.

All of this to be done with a short deadline, so that we can move this along, using existing technology, not inventing new technologies.

We think that this concept can be fleshed out. I'd like to just add, before I mention the characteristics of the network, that the larger problem in trying to achieve the balance that was described earlier is to not only have a network which encourages sharing but also to have the kind of guidelines and policy that encourage sharing; that we train people in sharing concepts and in classification concepts; and that we have metrics and auditing capabilities so we can see whether or not they're following the policy and guidance.

Mr. RUPPERSBERGER. And standards. You need standards.

Mr. CROWELL. Yes, and we need standards. We need compliance enforcement, both for protecting information that needs to be protected but also for sharing information that will benefit the public, the public good.

Just one last quick thing, some of the concepts that we believe are important then are concepts that have flexible access controls, authentication authorizations, so people trust the system; that they have a publish-and-subscribe capability in which people can say, I want to be able to get certain kinds of information to assist me in doing my mission or to assist me in doing my analysis, and they will get it; that it be a distributed system in which it's a system of systems. You don't build it centrally and manage it centrally from some place in the U.S. Federal Government. There's a longer list——

Mr. RUPPERSBERGER. I understand. We have other witnesses. I just want to make sure that we understand that we have done so much in identifying the problem; let's get to the implementation.

My yellow light has gone on so the quicker you can go, but I probably will not be able to ask you any more questions.

Mr. AFTERGOOD. Very quickly, a couple of points. The problem will never be fixed; it will never be over. It will always require continuing oversight, continuing refinement. Therefore, I would say, don't attempt to do too much. Do attempt to get the process started.

The other point I would just like to mention quickly is, when I hear trusted information network, I get concerned that, when barriers go down between agencies, they're going up between the Government and the public. So I would say keep in mind the question of public access. Keep in mind the option of allowing a way for the public to gain access to information that it needs sometimes.

Mr. RUPPERSBERGER. I would say this, we always sometimes have a tendency to overreact, and we still have to keep our eye on the ball and make sure that information, which can be very dangerous to this country or to the people working for this country, needs to be classified. And really there is an issue that hasn't been discussed, and I think if you can't trust the people with the information, then they shouldn't be in that position.

Ms. Haave.

Ms. HAAVE. The first thing that we have to do is to ensure that people are properly classifying information. What you find is, where there are seams, there's friction. So, as you're trying to create a trusted information network that spans the different Government agencies, local, State, etc., what we need are common standards and protocols.

For example, the Department of Defense and CIA have recently come to agreement on a metadata standard. Metadata is important so that computers can do for us what takes us a long time to do, and that is parse information with respect to security classifications in a way that people get the information that they are entitled to and not information that they're not.

Cross-domain security systems that allow accreditation across domains, not necessarily making one generic network, but having separate networks where the cross-domain security, that governance strategy, is already mandated and agreed to by all, will facilitate that movement of information across the network.

There are a number of things that we can do, automated tearlines, etc., and I think we are down the path of looking at doing all of those things. The DCI runs an Information-Sharing Working Group. There are number of congressionally directed actions that we are looking at with respect to that, and we are making progress toward that.

In the end, however, what it requires is that all of us come together with the common standards and protocols to facilitate that sharing, and that's an issue that's above any one Department.

Mr. LEONARD. Very quickly, sir, the one thing I would recommend being addressed is, as I alluded to before, the issue of unique agency prerogatives, especially those that are legislatively based. We currently have what I refer to as a patchwork quilt of various information protection and sharing regimes, not just in the classified arena but in the unclassified arena as well. We have literally dozens of unclassified—of protection regimes for controlled, unclassified information, many of which date back to the cold war, that we've never revisited. And we add to them every year.

We now have controlled critical infrastructure protected information. We have sensitive security information in the transportation field. We have sensitive homeland security information. All these are unique regimes that are being created and unique rules that are being written that will definitely impede when people then try to fuse all these various types of information in a network environment.

Mr. SHAYS. I thank the gentleman.

At this time the Chair would recognize Mr. Kucinich.

Mr. KUCINICH. Thank you very much.

I would first like to speak to the testimony of Mr. Aftergood. In part three of your testimony, you speak of the classification of the historical intelligence budget data, and you also get into the discussion, which Mr. Ruppersberger alluded to, about whether or not intelligence budgets ought to be classified.

This is not an arcane question or one that actually can be left solely to the Department of Defense or the Central Intelligence Agency. This is a constitutional matter. We take oaths, not to defend the CIA or the Defense Department; we take an oath to defend the Constitution of the United States. So to provide an appropriate frame for this discussion, let me cite Article I, Section 9, Clause 7 of the Constitution, "No money shall be drawn from the Treasury but in consequence of appropriations made by law, and a regular statement and account of the receipts and expenditures of all public money shall be published from time to time."

The Constitution of the United States makes it very clear, you can't have secret budgets. Our Founders anticipated that the only way to protect a democracy was to have it be open and that we know exactly how the taxpayers' money is being spent.

Now, I alluded at the beginning of this hearing to a book called The Sorrows of Empire by Chalmers Johnson. Here's what he says about this article, about Article I, Section 9, Clause 7 of the Constitution. He says, "This article is one that empowers Congress and makes the United States a democracy. It guarantees the people's representatives will know what the State apparatus is actually doing, and it authorizes full disclosure of these activities. It has not been applied to the Department of Defense or the Central Intelligence Agency since their creation. Instead, there's been a permanent policy of "don't ask don't tell." The White House has always kept the intelligence agencies budget secret, and deceptions in the Defense budget date back to the Manhattan Project of World War II and the secret decisions to build atomic bombs and use them against the Japanese.

"In 1997, then Senator Robert Torricelli, a Democrat of New Jersey, proposed an amendment to the 1998 Defense Authorization Bill requiring that Congress disclose aggregate intelligence expenditures. He lost, but he was able to make the point that the intelligence agencies spend more than the combined gross national products of North Korea, Libya, Iran and Iraq, and they do so in the name of the American people, without any advice or supervision from them," from Chalmers Johnson.

Now, I want to go a little bit more into this discussion, Mr. Aftergood. What about this? I mean, we are talking about something that is key to the survival of our democracy, are we not?

Mr. AFTERGOOD. We are talking about fundamental principles. It's easy to look at this, and think, oh, this is a detail, who really cares anyway. It's a fundamental principle.

Budget disclosure is one of only two categories of Government information whose publication is required by the Constitution, and as you correctly say, Government officials don't take oaths to particular agencies. They take oaths to uphold and defend the Constitution.

In this area, most Government officials have been derelict. I would add that it's not simply the White House. It's not simply the Bush administration. It's the Clinton administration. It's past administrations. It's the Congress. The last time the matter was voted on in the Congress in 1997, majorities in both the House and Senate voted against budget disclosure. I consider it a serious lapse.

I should say that the Constitution doesn't say that everything must be open and must be published right now. It says it must be published from time to time, and that allows the possibility that things could remain secret for a period of time. But when the CIA says that 50-year-old intelligence budgets must remain secret, that tells me that they are acting in bad faith. When the Justice Department defends the CIA, as they are doing now, in Freedom of Information Act litigation against having to disclose such historical information, that tells me they are also acting in bad faith and not in accord with constitutional values.

Mr. KUCINICH. Thank you.

I want to move on to Ms. Haave.

Today's headline, Washington Post, Iraqi Teens Abused At Abu Ghraib, Report Finds; Officials say inquiry also confirms prisoners were hidden from aid groups. The article goes on to say among other things that speaking on the condition of anonymity, because the report has not been released, other officials at the Pentagon say the investigation also acknowledges that military intelligence soldiers kept multiple detainees off the recordbooks and hid them from international humanitarian organizations.

Now, Ms. Haave, there have been several examples given today of instances where the Department of Defense has acted questionably in classifying information. These include large sections of the Senate Intelligence Committee's report on Iraq'sWMD program and the report of General Taguba on Abu Ghraib prison. Did your office make the decisions to classify those reports?

Ms. HAAVE. Sir, my office did not make those decisions. Original classification authorities make those decisions as documents are being prepared. The review for security declassification is also made by the original classifying authority.

Mr. KUCINICH. Now, this morning's Post that I just pointed out to you points that you have several of these new reports on the Abu Ghraib prison abuse; they're near completion. This one report by Major General Fay describes the use of dogs to attack and frighten detainees, including Iraqi teenagers.

So let me just ask you, for the record, will this report be made public, unclassified, in whole, and what about the report of the independent commission led by former Defense Secretary James Schlesinger that is also pending?

Ms. HAAVE. Sir, I have not seen Mr. Schlesinger's report, so I can't answer that question. With respect to the Taguba report, for example, I know there were places where information was classified, and there were other places in the report where that same information was not classified. There is a security review being undertaken today that should be done in the next couple of weeks, and so that security review and its results will be made available to you.

With respect to the General Fay report, I also have not seen that report in its entirety. I think large portions of it are unclassified, but again, I have asked, as a result of the interest in these reports, that the original classifying authorities go back and review and be sure that they are classifying properly those portions of the report that are classified, if they are.

Mr. KUCINICH. Have you ever been involved in keeping things classified as a way of protecting the administration from any embarrassment?

Ms. HAAVE. Sir, I have not.

Mr. KUCINICH. Now, these instances that we just discussed occurred recently in regard to operations in Iraq, Mr. Tierney pointed out earlier—and he and I have had the opportunity to work together on the issues relating to the testing at the Department of Defense—how you had results withheld from this committee for 8 months relating to the planned National Missile Program, and the report and all 50 recommendations it made were then reclassified,

though the report had been publicly available and disseminated before. Do you have any idea why this was done?

Ms. HAAVE. Sir, I don't. I only just learned of this instance yesterday when my staff brought it to my attention. What I am willing to do, however, is to go back and review it, pull the information as best I can and have a conversation with you about what the results are after I do an independent assessment. I know that's not probably satisfying to you.

Mr. KUCINICH. How long have you been involved in this particular assignment that you have?

Ms. HAAVE. In this assignment, as a deputy under, for about 1 year, sir, and then, prior to that, I was a deputy assistant secretary for security and information.

Mr. KUCINICH. Are you familiar with the challenges which this committee made to the administration over gaining access and public release of materials with respect to the Missile Defense Program?

Ms. HAAVE. Sir, not always. Typically, what happens——

Mr. KUCINICH. Is that a yes or a no?

Ms. HAAVE. Sometimes, I am. For example, with respect to Abu Ghraib right now, I am aware of those things.

With respect to missile defense, what happens is that the original classification authority, which in this case is probably the Missile Defense Agency, would handle those. I would not necessarily be apprised of those.

Mr. KUCINICH. Do you have any oversight over them at all? Do you look at their classification decisions?

Ms. HAAVE. We do have oversight over the Department. Most of that is conducted at multiple levels, decentrally, and so they have a responsibility to assure that their people are properly trained. They have a responsibility to conduct self-inspections and to report. We often will answer questions for them, and we sometimes go and visit. I cannot remember the last time that we had a conversation on this subject with the Missile Defense Agency.

Mr. KUCINICH. Mr. Chairman, the question that I think needs to be asked here is, who has the final word on classification? I mean, you can chase this thing around a tree forever. Who has the final word on classification, let's say, on the Missile Defense Program? Do you have the final word or don't you?

Ms. HAAVE. No, sir. The Missile Defense Agency has the final word, to the best of my knowledge. What we have done inside the Department, that is a recent change, for example, with respect to the habeas cases at Guantanamo is that we have convened a group of people, for example, from Guantanamo, from SouthCOM, from the office of the Secretary of Defense in order to take on these classification/declassification issues. And where there are impasses, where people cannot come to agreement, those things will now be brought forward to me, and I will make the final classification decision. That is new in the Department of Defense.

Mr. SHAYS. At this time, the Chair would recognize Mr. Tierney.

Mr. TIERNEY. Thank you, Mr. Chairman.

Ms. Haave, I don't mean to pick on you, but I do want to follow-up on this line of thought. First of all, I'm grateful for your offer

to look at that information and get back to us. I presume you will do that within a week or two.

Ms. HAAVE. Yes, sir, I will.

Mr. TIERNEY. I'll tell you why, because I think the public needs confidence that this classification system is not being used for political purposes, that it's not being used to demonize somebody or to avoid embarrassment. We have serious issues here, and they are how we're going to apportion our resources and whether we're going to apportion them fighting the cold war and looking backward with a National Missile Defense System that's unproven and untested, or whether we're going to acquire resources for the most immediate threat according to our own intelligence agencies and almost every other independent body that has looked at what our needs are at this point in time.

You heard my rendition of how we press this matter, and I want you to know that Mr. Waxman, who is the ranking member of the full Committee on Government Reform, and I sent a letter as far back as March 25th of this year, March 25th to Secretary Rumsfeld objecting to his reclassification of already public information, as well as his classification of a report based on that.

And essentially, we found that this is important information. What he is doing is preventing a public debate on this. We can always debate whether that's a system that's necessary or not, but we do need a debate on whether or not it should be going to the field unproven or untested and how much money we are going to spend or how we're going to spend $10 billion. And that's something that the American people need confidence that those decisions are being made.

He has not responded yet. So you should know, we can give you a copy of that letter, but since March 25th, they haven't had any hesitation in going forward and saying that they're going to deploy this system and making a big political hullabaloo about it for those that they're interested in satisfying, but they haven't found time to respond to, I think, very legitimate instances.

Let me share with you one other aspect you may want to investigate when you look at this. Theodore Postol is a Professor of Science and Technology and National Security at the Massachusetts Institute of Technology. At one point in time, he wrote a letter to the White House that described how the Missile Defense Agency had doctored results of the National Missile Defense test to hide the fact that they could not tell the difference between simple decoys and warheads. He described how the Agency had altered its entire test program to hide that flaw.

Subsequently, two General Accounting Office reports issued in March 2002 verified the facts that he had written about to the White House.

The way the Agency responded to that was by claiming that it was classified. What it did beyond that was it then sent three agents to deliver a letter to Mr. Postol that was classified as secret. The letter contained nothing more than publicly available information deemed classified by the Government, in his words, so that the Agency could claim that he would be violating security agreements if he continued to speak on the matter of national security. That's pretty extraordinary.

That's going to a pretty extreme length, and that's just not a matter of oversight for somebody making a bad decision about that. That's a conscious decision to try and muzzle somebody who had very specific and worthwhile information for the public to know and for us to make determinations on how we're going to allocate our resources.

So I hope you will also look into that matter. We can send you some information on that. Will you do that?

Ms. HAAVE. Yes, sir.

Mr. TIERNEY. Thank you. That should make every American concerned about just how these decisions are being made.

So with that in mind, and I note, Mr. Aftergood, you had a very nice thought in your report that congressional oversight is necessary and important, but you say it need not be arduous or an elaborate undertaking; it can be as simple as posing a question to the Pentagon. That's not so. We have been posing this question for years and getting stonewalled on it.

So I think what we might discuss here is beyond—now, that's the way Government should work and that's the way we'd like this administration to work. They clearly are not working that way, given the lengths to which they go to get Mr. Postol quieted and the fact that we haven't had an answer from March 25th. It took us to 2000 to get this information first to the public domain and then reclassified.

What's a better way for congressional oversight—and that's the question I pose to each of the members of the panel—after we have the challenge or the classification determination made within the administration by the Interagency Security Classification Appeals Panel, ISCAP, which is nothing more than executive officers looking it over, although they have had a pretty good record of ordering some declassification that's not a 100 percent when they don't agree with the public, when the public raises a question about reclassification, and as to declassification, where do they go? What should be Congress' role? How do we get some decent oversight that sticks to what we are trying to do here and not go beyond that?

Mr. Leonard, I'll start with you and maybe go left to right.

Mr. LEONARD. If I understand your question correctly, sir, is, where would the public go after, for example——

Mr. TIERNEY. Well, when Members of Congress who says we'd like have this declassified, the executive says no, then you have Mr. Aftergood's recommendations, have a nice letter saying, please reconsider and let us know what your thoughts are, and they basically send you off into ether space somewhere.

Mr. LEONARD. Basically, pursuant to the order right now, you've identified one of the two primary routes individuals have. One is to go through the courts, through the Freedom of Information Act process.

Mr. TIERNEY. What's the record been on that? Is anybody familiar with any court——

Mr. LEONARD. My understanding is that almost without exception the courts will always defer to the executive branch.

Mr. TIERNEY. Exactly.

Mr. LEONARD. And the other process that you alluded to, that's provided for in the Executive order, is to go to this administrative appeals process, to this interagency group which does have at least somewhat of a more favorable record with respect to releasing the information.

My experience has been that, when a group of agency representatives get together rather than just the owner of the information, you get a less parochial view of the situation, a more holistic assessment, and I believe, off the top of my head, the historical record is that, approaching 60-some odd percent of the time, the panel will override an agency's determination in whole or in part.

Mr. TIERNEY. I appreciate that account.

Now, we get to the point where, in instances, the decision back to thepetition, whether it be a Member of Congress or a member of the public in general, is unsatisfactory, Congress should have a role to play here. That's our oversight responsibility. We've had hearings here. We get stonewalled left and right. So what you're saying, our only response is to subpoena and beat it out of them, and in that sense of the word, ought there to be some statutory change? What's your opinion where we should go from here?

Mr. LEONARD. The challenge there is that, by and large, the exercise of classification authority has primarily been pursuant to the President's constitutional Article II authorities, and that, of course, would complicate any sort of legislative remedy with respect to ultimate decisions along those lines.

Mr. TIERNEY. So you're saying, nowhere, we're stuck?

Mr. LEONARD. I do believe that there can be more responsive means by which to resolve disputes. I believe the ISCAP process can be enhanced. I believe——

Mr. TIERNEY. How would you do that?

Mr. LEONARD. One of my concerns is the ISCAP process right now is primarily—and I'm not trying to be disparaging here—but is primarily a hobby horse for historical researchers. And again, that's important that they get that kind of information, but I believe that process can be used for more relevant, more timely information as well, and I believe it can be stepped up, possibly with some sort of specific time limitations for action and with consequences if action is not taken; for example, absent of a decision, such and such would occur. Those types of remedies at least provide for a responsiveness and provide for some consequences if attention and resources are not devoted to that topic.

Mr. TIERNEY. Ms. Haave, since that's in a Presidential Executive order, would you recommend to the President that he take that kind of action and step it up, as Mr. Leonard says, or what would be your remedy for Congress and the American public?

Ms. HAAVE. I think there are a number of things that we can do that are different from how we've been doing this in the past. The first step I just described, within the Department of Defense, for this limited classification review for these reports, but that's not to say that we shouldn't put in place a process whereby that information comes to me or comes to whoever sits in my position or in a different position as decided by the Secretary and is an adjudicator within the Department. That may, in fact, facilitate and speed some of the questions and answers that you appear to want.

I think the ISCAP could, in fact, be expanded a bit beyond its typical historical base to do those kinds of adjudication when the Congress is feeling that it's not getting the information that it needs.

On that committee sit representatives from each of the agencies. We review the information that's in question. We research it, and we make our decisions. And that could, in fact, for your information, be provided to you.

Mr. TIERNEY. Is my understanding correct that right now ISCAP does not do that? For instance, if the Secretary ever decided to respond to our March 25, 2004, letter, and we wanted to appeal that to ISCAP, we'd be thrown in the pile and maybe never reached at all.

Ms. HAAVE. Mr. Leonard could probably answer this. I don't know that the Congress has ever come to ISCAP and asked for that.

Mr. LEONARD. There's no reason why that could not be processed according to those procedures.

Mr. TIERNEY. With respect, of course, that then those executives, which would include the Department of Defense Secretary, would then want to respond from that body where they haven't responded individually.

Mr. LEONARD. That's correct.

If I could make one further point, Mr. Congressman, that I neglected to make. There is currently on the statutory books since 2001 a Public Interest Declassification Board. This is an outgrowth of Senator Moynihan's Secrecy Commission. It was his legacy. It does exist on the books, as I say.

The administration has taken action to look to appointing some members, but quite frankly, there has been no action from the legislative branch that I'm aware of to appoint their members. And this is an existing forum that does exist that will allow for some of these issues that you addressed to be worked out in such manner.

Mr. TIERNEY. Thank you.

Mr. Aftergood.

I'm taking license here, Mr. Chairman, for the last two of these. Thank you.

Mr. AFTERGOOD. There's a pending proposal that's been introduced in the House and the Senate. In the House, it's H.R. 4855, to create an independent National Security Classification Board, which I believe is intended to serve as a forum to mediate these kinds of disputes. In several ways, it really replicates the Public Interest Declassification Board that Mr. Leonard mentioned, but it's something that's maybe worth considering.

To answer your question directly, what to do, I think look at what works and strengthen it. ISCAP works on a small scale. It has led to the declassification of all or part of the majority of disputed cases it has worked on.

ISOO, Mr. Leonard's organization, if he will forgive me, works. A couple of months ago, I faxed him, Mr. Leonard, a letter pointing out the Taguba report seemed to be improperly classified. He responded to me the very same day, initiating an investigation and carrying on some work he already had underway. I thought it was

an extraordinary response from a Government agency. Nobody responds like that.

But ISOO is a tiny organization, particularly when it's compared to the vast expanse of the Government classification system.

But look at what works and strengthen it. I would even say that your questions that have been stonewalled are not without effect. I don't think Ted Postol would say that you have accomplished nothing. I would think he would say you have accomplished a great deal by standing up for his interests over a period of years.

Regular hearings are very important. I think, perhaps when Mr. Leonard's organization puts out his annual review of the classification system, it might be an opportune time to hold regular oversight hearings on what's going on in the classification system, what's going right, what's going wrong.

Harness the courts. The scope of judicial review has shrunken over the years to the point that courts now routinely defer to executive branch agencies. They say, if you say it's classified, that's all we need to know, we're not going to look further. That is not what Congress intended when it enacted the Freedom of Information Act. I think if there is the political will, it would be very desirable if Congress could say our intention is that the courts do real review of classification decisions. That doesn't mean overturn them all the time. It means look at them and see if they make sense. Do not defer. Exercise your judicial function. If that can be accomplished, then a great deal will have been done.

Mr. TIERNEY. Thank you.

Mr. Crowell.

Mr. CROWELL. Mr. Tierney, I think, in fairness to the Markle Foundation, I should say that they have not studied this issue, and I cannot represent them on it, but I do have personal views.

Mr. TIERNEY. Well, let me hear your personal views.

Mr. CROWELL. First of all, I participated in the Commission on Secrecy that Senator Moynihan conducted, and as a result of some of that participation, I have seen large numbers of Government documents released and declassified.

My personal belief is that we have to start with the policies that currently exist and the guidelines that currently exist at the department and agency levels, and we have to refine them and redefine them in some ways in which we emphasize what needs to be released to the public and what must be shared with other agencies in order to conduct the fight on terrorism, as opposed to the current mechanism which is owing it toward what must be protected.

Second, guidelines that are completely inconsistent with those policies should be developed in each agency. Each agency has a unique problem that they have to deal with in terms of substance and so on, but they should be refined even further to—and issued in each agency and then reviewed by those departments to make sure they are consistent with the policies of release and of sharing.

Third, there should be metrics and audits that are conducted, as many of them as possible conducted in automated means, which means that you actually look at trends that were discussed here by the committee, and each agency expected to review those audits and those trends and make reports.

Finally, there should be a compliance mechanism which says, here are the consequences of not following these policies.

And I said finally, but I think the final thing is that there should be reports to Congress which essentially say how the policies and guidelines are being followed and how consistent the practices and conformance is across the entire Government. I think that's at least a fair way in which we can approach the problem.

Mr. TIERNEY. That's very helpful.

I thank all of you for your testimony.

Mr. SHAYS. I thank the gentleman.

I want to just first start out by saying, I have this impression that the President's in charge, and then it degenerates into 4,000 people who then make the decision. I used the word degenerate, but I mean, in other words, it goes down to 4,000 people. Is that a right impression or a wrong impression?

Mr. LEONARD. The one thing I would modify that with, Mr. Chairman, is the critical role that agency heads play. The President, in his executive order, directs agency heads to take personal involvement to ensure the commitment of senior management.

Mr. SHAYS. So how many people do we think it would be? In other words, if the President wanted to delegate to one person and say we need to change this and I want to get everybody together, you're not going to get 4,000 people together. How many people would the President need to get together with?

Mr. LEONARD. You would need to get together those agency heads with original classification authority, as well as especially those agencies with other unique statutory or regulatory authorities in this related area. You're talking dozens. I can't give you an exact count, but it is——

Mr. SHAYS. It would be just dozens?

Mr. LEONARD. I'm sorry, sir.

Mr. SHAYS. It would just be dozens? It would be under 100?

Mr. LEONARD. Yes, sir. I firmly believe that those 4,000 original classifiers can respond very effectively to the leadership of their individual agencies. That's where the tone is set. That's where, that's where——

Mr. SHAYS. Let me say, where I think the tone is set is at the very top, and I have this general view that most Presidents, but particularly this administration, believe that the less known, the better. I happen to believe the more known, the better. I think they draw on experiences of past Presidents, Iran Contra, you go through this list of it, and there's this general view that I hold that you don't talk, you don't tell, you don't discuss, you don't disclose. That's a view I hold as a Republican about, frankly, a Republican administration.

At any rate, the tone is set to the agency heads, and you believe that, ultimately, agency heads set the tone for the various people, the 4,000 people that work under them.

Mr. LEONARD. Absolutely, sir. Secrecy is an important tool, especially in time of war, but it is a tool that comes at a price.

There's a consequence to secrecy, and my frustration is that I do not believe that this Government, through its agencies, consistently approaches the issue of to classify or not as a deliberate process,

as an informed process; that secrecy in some quarters is almost a fundamental first response.

Secrecy can be a fundamental issue, and it should be. It's a fundamental tool, but it should never be an automatic first response, because there are consequences to it, and that's what we have to instill, from my perspective, a more informed and more deliberate process in terms of to classify or to not.

Mr. SHAYS. Let me get into that in a second, but Ms. Haave, do you disagree with the general view that it's the President down to agency heads and then 4,000 people?

Ms. HAAVE. Clearly, there's a framework that we work to that is executed by the agency heads through the Department. I will say that, with respect to a number of the reports that are coming out now and because of the interest in them, that the timeframe by which we would do these security reviews normally has been shortened, and in fact, the Department has had actually a good history of declassifying large amounts of information. In fact, the Under Secretary of Defense for Policy has initiated a tiger team, if you will, to look at documents pertaining to pre-Iraq and Afghanistan, as to whether or not they can now, in fact, be declassified.

So I think there is no doubt that, at the top, the tone is set, and I think that is executed through the Department. We have somewhere on the order of 2 million cleared personnel. That's equivalent, roughly, I think, to the population——

Mr. SHAYS. What's that mean?

Ms. HAAVE. People who have clearances, confidential, secret, top secret. That's roughly equivalent, I think, to the population of the State of Rhode Island. So it's not an inconsequential effort that we go through, the way that the Department does it, that it's decentralized.

Mr. SHAYS. I don't know what that says to me. You're saying, 2 million people can look at classified documents. How does that relate to the issue of overclassification?

Ms. HAAVE. What it says is that how we conduct our training, how we conduct our oversight, we probably are the largest organization that has classified information.

Mr. SHAYS. I understand, but I don't gain any comfort from that or not because, once something is classified, I don't have the right to talk about it.

Ms. HAAVE. Correct.

Mr. SHAYS. I don't have the right to talk about it. I have oversight of the Department. I can't talk about it, and I have 17 years now of experience and some huge disagreements with your Department, and, I mean, my own Government's Department of Defense.

I'm grateful for what the Department of Defense does. But I can go back to 1991 where I had an Inspector General who said they classified a study. Our study was that we had determined that 40 percent of the masks were basically leaking. These are the chemical masks, and nobody's doing anything about it, and it's classified. So they came to me. I went to Senator Riegle at the time, who also knew about this, to say, what do we do about this? And there was this play on two different parts. One is we didn't want to disclose.

First off, the Army disagreed that they were vulnerable and that they leaked. So we debated for 6 years on whether the Inspector

General's report was accurate, which for the most part was, and we had this issue of, well, do we declare that we're vulnerable. But then I had this knowledge that the men and women who were putting these things on were putting on masks that didn't basically work. They didn't know it.

Now, the Department was saying, well, it's still a debate. It didn't seem to me we should have debated for 6 years whether this Inspector General's report was valid, and yet we finally outed this report when we started to talk about Gulf war illnesses because it happened to relate to it, and then it was made public by the Department of Defense. They put it on the Internet, and then they took it off.

I mean, that's just one experience that I've had, and frankly, I just, for the life of me, don't know how to have dealt with it. I couldn't disclose it, and yet I knew about it.

I'd like to know—Mr. Aftergood first, why don't you just start—is this a President to executive heads to potentially 4,000 people?

Mr. AFTERGOOD. My perception is that it's the agency head level that is the most important, perhaps even more important in some ways than the President. If you look back over the past decade, what you see is that openness and transparency flourish where the agency head cares about the subject and wants it to happen. They care about it, it happens. If they are indifferent, it doesn't happen.

In the Clinton administration, we had former Energy Secretary Hazel O'Leary who, in fact, got way out in front of her own administration with an openness initiative. Some people said she declassified to a fault. I don't necessarily agree with that, but the point is, she cared about the issue. She made it a priority. It happened, even over the resistance of her own agency.

In the first Bush administration, DCI Robert Gates had his own modest openness initiative in the intelligence community. It's the agency heads who really make stuff happen.

Mr. SHAYS. I don't want us to be naive. I don't want us to be foolish, but I just really believe when I look at the documents that I've seen, my number comes closer to the 90 percent overclassified than the 10 percent because I would tell you, page after page, slide after slide, I would look at the Army folks, the Marines, the Air Force, the Navy folks who would give these briefings, whether in Iraq or anywhere else, and I'm saying, is this classified? And it would have, you know, some classification, and I would be dumbfounded as to why. Collectively, when I start to think about it, I can hardly think of a few things that I felt were classifiable material.

Let me ask you, Mr. Crowell, your view of the President, the agency heads and then the 4,000. Is that the way you view it?

Mr. CROWELL. Again, this is a personal answer and not reflective——

Mr. SHAYS. Yes, it's an answer based on the fact that I read your bio.

Mr. CROWELL. I have gotten the experience.

Mr. SHAYS. Yes, you have a hell of a lot of experience, and that's not secret.

Mr. CROWELL. I would agree, first of all, that the overall tone is set in policies that come from the Presidents to Departments, but I would also agree with the members of the panel that the agency

heads really set the tone for what happens on the day-to-day basis, on whether or not people are properly trained, properly oriented and whether or not there are any consequences whatsoever for classifying something improperly.

Mr. SHAYS. Let me do this. Let me ask this one other question, then go to Mr. Tierney.

You get the quote for the day, Mr. Leonard. You said, for example, "it is no secret that the Government classifies too much information."

What is a secret to me is whether it's 10 percent or 90 percent. I'm going to ask each of you to give me your best estimate of whether you think we classify, overclassify too much to the level of 10 percent or closer to the level of 90 percent. I'm going to give you an opportunity to answer last. You had the quote of the day.

Mr. Crowell, I want you to give me the answer. What is the secret to me is whether it's 10 percent or closer to 90 percent.

Mr. CROWELL. In all fairness, Mr. Chairman, I have to put some context around the question. I realize you framed it carefully. I'd like to frame the answer carefully.

I believe, with regard to advanced technologies and weapons systems and so on, it would be more favorable to proper classification initially, but it would remain classified for a longer period of time than most people might consider appropriate when you look at the pace of technology today.

Mr. SHAYS. So, on the technology side, you would be closer that we overclassify over 10 percent or less, but over time, it's still classified, and then you could maybe make the argument that it is closer to the 90 percent over time?

Mr. CROWELL. That's correct, sir. With regard to sources and methods in the intelligence field, I would have the same general, although I'd make it an 80/20 cut.

Mr. SHAYS. At the end?

Mr. CROWELL. Yes. It would be 80 percent properly classified to protect a source or a method in the beginning, and then over time that source and method goes away and it doesn't get declassified.

Mr. SHAYS. And it should be, in your judgment.

Mr. CROWELL. With regard to information——

Mr. SHAYS. It should be—over time be declassified.

Mr. CROWELL. Yes. With regard to information, that is the essence of conclusions either of analysis or whatever, I think it tends to be overclassified quite heavily because people fear that sources or methods will be revealed when, in fact, if they did their own careful analysis, they would find that a lot of information, just set as information without saying where it came from and who produced it, would be unclassified.

Mr. SHAYS. You know what, this is a longer answer than what I am expecting.

You want to jump in?

But they're good answers. It's not a reflection on you, these are excellent helpful responses. Mr. Aftergood.

Mr. AFTERGOOD. My personal access to classified information is very limited and entirely unauthorized. I don't feel qualified to answer that in any detail. I would say that your question is predi-

cated on a correct assumption that classification decisions are subjective.

Mr. SHAYS. Could I ask you a question? Based on your answer, are you saying you're like Woodward, you just basically get all this information but——

Mr. AFTERGOOD. That's not the way I would put it, but I would say sometimes I stumble on stuff, sometimes people send me stuff. That's just the way it is. Classification is a subjective matter. You know, I might have my opinion, others will have their opinion. What do you do about it? I think if there are 4,000 people in the executive branch who are out there classifying information, maybe we need, if not 4,000, then at least dozens of individuals or entities distributed throughout the executive branch whose job it is to oversee and to look for overclassification, many ISOOs planted throughout the executive branch that function like antibodies to counter inappropriate classification. Just as classification authority is widely distributed, maybe we need to find a way to widely distribute declassification authority, people whose only job is to look for overclassification.

Mr. SHAYS. OK. You're getting to me like Alan Greenspan, you're talking in tongues a little bit for me. My original question was the 10 percent/90 percent.

Mr. AFTERGOOD. And my original answer was I don't know.

Mr. SHAYS. But you used that as a wonderful opportunity. I didn't catch on right away.

Ms. Haave.

Ms. HAAVE. I agree with that. I don't know.

Mr. SHAYS. No, you do know. You do know more than most.

Ms. HAAVE. I do believe that we overclassify information. I do believe that it is extensive not for the purpose of wanting to hide anything, but I will tell you that with respect to military operations, people have a tendency to err on the side of caution and so therefore may in fact classify things, and at the time they could, in fact, be classified. Military operational data tends to be perishable. So after the operation much of that can be declassified.

There are clearly things that will continue to take place in an operational environment that we do not want to release. And those are—you know, have to do with sources and methods and——

Mr. SHAYS. So you're basically saying it's greater than 10 percent, but you're not suggesting how much greater.

Ms. HAAVE. How about if I say 50/50?

Mr. SHAYS. OK. That's significant. Someone in your experience would say we tend to do it 50/50. I think that's quite significant. Thank you.

Mr. Leonard.

Mr. LEONARD. Two approaches. One is information that shouldn't be classified in the first place is ineligible to be classified. That's a number that, quite frankly, from my perspective over the past year, is disturbingly increasing, where information is being classified that is clear, blatant violation of the order.

Other than that, as Mr. Aftergood pointed out and as I pointed out in my testimony, this is an act of discretion. It is an application of judgment by an original classifier. To give some empirical basis to my answer, I serve as the executive secretary for the appeals

panel. And at least in that environment, in those instances where the panel still votes to uphold the classification, based upon my over 30 years of security and counterintelligence background, my personal opinion, my personal judgment, is even that is overclassified. And so from that point of view, I would put it almost even beyond 50/50 in terms of when it comes to applying judgment, there's over 50 percent of the information that, while it may meet the criteria for classification, really should not be classified in terms of what we lose. The price we pay for classification outweighs any perception, any advantage we perceive we gain.

Mr. SHAYS. Mr. Tierney.

Mr. TIERNEY. Thank you.

Ms. Haave, when a document comes from the Department of Defense and is marked on it "For Official Use Only," who creates that designation and what exactly does it mean?

Ms. HAAVE. "for Official Use Only" is not a classification level. It's an exemption, if you will, from public release for certain types of information that may have to do with privacy, it may have to do with proprietary information, it may have to do with law enforcement information. There are categories of information. "for Official Use Only" does not mean, however, that is releaseable to the public.

Mr. TIERNEY. So let's take an example of the situation where a director of operations, in testing an evaluation, issues a report that he is required by statute to make, comes before the Government Reform Committee and testifies orally as to the content of that report in significant detail without objection from the Department of Defense. There are charts, there is written testimony, it's on C–SPAN, it's recorded and replayed on C-span. That information is put on Web sites, remains on Web sites for an extraordinary amount of time. Groups like the Union of Concerned Scientists and other outside experts review the information and put opinions out with respect to it.

And then months later, in answer to a request of this committee that the report be issued out, all those things being in the public domain for almost a year, the committee gets a document saying "For Official Use Only." How does that fit in with the classification or with the description that you just gave me? What category does that fall under?

Ms. HAAVE. Without knowing the substance of the report, sir, it's hard for me to—and I won't look at the substance of the report.

Mr. TIERNEY. Well, I can tell you the substance of the report was public for almost a year, but it was publicly stated it is a statutory report.

Mr. SHAYS. Will the gentleman suspend? Let me tell you this is the challenge that we face as a subcommittee. Part of our responsibility is to—in the context of a public hearing—is to disclose what we've learned. When we get documents "For Official Use Only" we don't know if that's classified or not classified. Frankly, the way I treat it is you would prefer whoever sends it that it not be publicized, but we have every right to publicize it. That's kind of the way I interpret it.

Mr. TIERNEY. With all due respect, it goes beyond that for me, as you know. It's to the point of ludicrous. When you put it out

there in the public domain for that, the Department does not object to its—nobody came in and said this individual shouldn't testify. It's a statutory report. Then to try and put some sort of designation, which admittedly is not a classification, smacks to me of just an attempt to put this on and hope they don't put it out, because we'd like to keep it secret, and then some years later when that information is used for the foundation for a very critical report on something that a group of people want to politically do, it's classified retroactively. That's the challenge.

I don't expect you to answer this now. I don't want to be unfair to you or anything like that. But that's the challenge I want you to take back with you on that. Because that is an insult to the American people, to the public, to this institution of Congress which continually struggles with the way in which it's going to do its oversight. If I have to be critical of all the things with this particular Congress, the last of this 108th, 107th, it's an absolute abdication of our responsibility for oversight. A lot of it is not the fault of Congress but the fault of a totally uncooperative administration that will not be forthcoming and will not cooperate and will not work with Congress to allow it to do its job and feels that the executive—the prerogative surpasses any responsibility to Congress and doesn't allow or want Congress to do its constitutional functions.

I think we've got to redraw that balance. Congress has to have the ability to have oversight. It should be strong oversight if we're going to have a successful government here, particularly in view of the 9/11 Commission Report.

If we have, as we do have, the challenge of homeland security and protecting these people or whatever, and if we want to give more authority to a national intelligence director and to a center on counterterrorism, then we had better have an equally aggressive congressional oversight, or it's going to lead to an executive that is out of control, taking this country in a direction we may not want to go. So it has to be corresponding—for to us do the job we need to do against terror, we have to have that national intelligence director, I believe, and a counterterrorism center. But that only works if, correspondingly, we have a strong congressional oversight authority that goes in line with what our constitutional responsibilities are, and that means getting this issue of classification under control and not having that kind of a situation where you get "For Official Use Only" nonsense sent up here after it has been in the public domain, and then a reclassification just because a report is critical and doesn't let you go off in some ideological path here to try to satisfy one element of your supporters on that.

So I thank you. I won't ask you for an answer on that because it really was more rhetorical than anything. But please do get us your review of that. Let us know. We do need to get the bottom of that particular issue.

Thank you, each and every one of the witnesses, for the valuable contributions you have made here today.

Mr. SHAYS. I agree with the gentleman. You have been a wonderful panel and very helpful.

I am going to ask another question that I am wrestling with. I don't expect necessarily I'm going to get definitive answers. But in

my capacity of chairman of the National Security Subcommittee, we oversee Defense, State Department, and the Department of Homeland Security, for programs, waste, abuse, fraud, how well are they running the program and how well they are not. So we have a keen interest in the notification system. The country has been at yellow, which is elevated alert. Everybody thinks we've just been at general alert, because that's the way we feel. But we're at elevated. When we kick into orange, which is high alert, that's quite significant.

We kicked into high alert last December, and we kicked into high alert because we were basically told planes might be hijacked from Europe to the United States and a concern that at a high-profile event a dirty weapon might be used. Now, there was more detail to that. The public had a general basis to understand it was something like that.

So when people called and asked should their kids fly to Europe during Christmas when they heard we went to orange, I said well, I wouldn't have my daughter fly to Europe because she'd have to fly back. The flying back was the concern.

When I had groups say, well, if we went to an event like New Year's Eve in New York, would it make sense to bring my kids? I said, well, I sure as heck wouldn't bring my child. In fact, I would think twice before going because it is at a potential target.

Now, in the process of having Admiral Loy come before us, the Deputy of Department of Homeland Security, I asked him what was the threat? He said to me, I can't disclose this in an open forum, and I am thinking to myself, let me get this straight: The terrorists know that they're going to hijack a plane and the terrorists know they want to do the following, and the government knows, but the public doesn't know that may go to those venues.

I just find that absurd to the point of wondering how could he have said no. He did say no. He said no more than once when I requested it. Walk me through his best argument as to why he would say that. It may be a very good one, and you can wipe the smile off my face, but tell me the best argument that you would know for not disclosing this information when the terrorists knew and the committee knew and certain privileged people knew.

By the way, I want to say this to you. Every staff person and every Member who got that briefing told me they wouldn't fly to Europe and they wouldn't go to a venue like New Year's Eve in New York. So they knew. The public didn't know, and so tell me the best argument here.

Mr. LEONARD. Without knowing the specifics myself, sir, the best argument that I could articulate is concern possibly that what we knew, how we knew it, the specificity that we knew it, and whatever might reveal sensitive sources and methods that was used to collect that information.

At the same time, though, I would like to make one very important point. As you know, the President amended Executive Order 12958 just last year. One of the things we specifically included in that order was that when it comes to homeland security, when it comes to imminent threat to life or to property with respect to homeland security, and there is classified information that individ-

uals need to have, the absence of a security clearance shall not serve as an impediment to the sharing of that information.

Mr. SHAYS. So, for instance, if the chief of police of New York needed this information, he could get it.

Mr. LEONARD. Exactly. Just a couple of months ago I had a rather senior official come up to me and say—this was post-Madrid bombing—he said, I was in this environment, I had some senior private sector individuals there, I was telling them what they needed to do post-Madrid, they wanted specifics; I felt compelled that I had to give them specifics, so I disclosed classified information to them.

The reason he was bringing it up to me, he turned to me, he said, Leonard, am I going to have problems with my polygraph the next time I take one? I was able to assure him absolutely not, because that is exactly what that revision of that policy was intended to address, those types of situations.

The challenge now for agencies—and not all agencies are there—is to implement this provision within their own implementation regulations so as to empower their rank and file to be able to have that same confidence. He did it not because he knew about the policy, he did it because he had the rank that gave him the confidence. But we need to empower people. That was the intent behind that policy revision. It was very important, and we need to move out on implementing it.

Mr. SHAYS. Thank you for sharing that. Is there any question we should have asked any of you that you might have prepared that for, that you think needs to be part of the record? Frankly, sometimes that question elicits some of the most important information we get from a hearing. Is there anything that we need to put on the record, anything you feel guilty about that wasn't.

Mr. AFTERGOOD. I might add one quick thing. This whole subject has been investigated by a congressional commission led by Senator Moynihan, the Commission on Protecting and Reducing Government Secrecy. They took a year or more, couple of million dollars, produced an excellent report, a whole series of recommendations. It essentially went nowhere.

I think one of the lessons of that is that one should not be overly ambitious in trying to fix this whole problem at a single blow. And that's why I think it is of particular importance that the 9/11 Commission recommendation to start with intelligence budget declassification is such an astute one, because it is a finite, specific, achievable goal that will have positive consequences throughout the system.

Mr. LEONARD. If I could reiterate one point, Mr. Chairman—I alluded to it before—but speaking of Senator Moynihan again, there is his legacy, the Public Interest Declassification Board. That is legislation that was passed several years ago. It's on the books. It's never come to fruition. I personally would urge you, to the extent you can, to confer with leadership in the legislative branch to see if there's a way to move forward with that. It's not a silver bullet, it's not a solution, but it is a tool that's out there right now that provides for legislative executive branch interaction on this issue. And I know from my understanding, I believe the executive branch is ready to make some nominations to serve on that board.

Mr. SHAYS. That's interesting as well. Thank you.

Ms. HAAVE. I also would like to say that I think the discussion really needs to be about risk and how much risk we're willing to take. For example, if another organization has information that is relative to the Department of Defense and the protection of lives, and we would like to have that information released to protect our forces, is it that one person could be saved, 10 people could be saved, 100 people, 1,000, 10,000? At what point does that risk decision come into play and how do we make that risk decision in the best interest of the Nation?

Mr. SHAYS. Yes. OK. Thank you. Mr. Crowell, did you have any?

Mr. CROWELL. I would just like to underscore some of the things that were said earlier about the contributions of Senator Moynihan and his Commission on Secrecy, but also about the book he wrote afterward which was called "Secrets," which is a remarkable study of the history and the impact of decisions that have been made by people throughout history, both positively and negatively on the country and our well-being.

Mr. SHAYS. Thank you very much. I also want to thank Mr. Leonard, Ms. Haave, as government officials to be able to have you sit on the same panel with nongovernment officials, it helps us do our job better. I appreciate you not making that an issue. This was really a very interesting panel. I learned a lot. We got our work cut out for us but I think it's important work. I thank you all for the work you all do. Thank you.

With that, this hearing is now adjourned.

[Whereupon, at 12:17 p.m., the subcommittee was adjourned.]

○